

3Com® Switch 7750 Family
Configuration Guide

Switch 7750
Switch 7754
Switch 7757
Switch 7758

www.3Com.com
Part Number: 10015462 Rev. AD
Published: December 2007

3Com Corporation
350 Campus Drive
Marlborough, MA
USA 01752-3064

Copyright © 2006-2007, 3Com Corporation. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3Com Corporation.

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a "commercial item" as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com and the 3Com logo are registered trademarks of 3Com Corporation.

Cisco is a registered trademark of Cisco Systems, Inc.

Funk RADIUS is a registered trademark of Funk Software, Inc.

Aegis is a registered trademark of Aegis Group PLC.

Intel and Pentium are registered trademarks of Intel Corporation. Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation. Novell and NetWare are registered trademarks of Novell, Inc. UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd.

IEEE and 802 are registered trademarks of the Institute of Electrical and Electronics Engineers, Inc.

All other company and product names may be trademarks of the respective companies with which they are associated.

ENVIRONMENTAL STATEMENT

It is the policy of 3Com Corporation to be environmentally-friendly in all operations. To uphold our policy, we are committed to:

Establishing environmental performance standards that comply with national legislation and regulations.

Conserving energy, materials and natural resources in all operations.

Reducing the waste generated by all operations. Ensuring that all waste conforms to recognized environmental standards. Maximizing the recyclable and reusable content of all products.

Ensuring that all products can be recycled, reused and disposed of safely.

Ensuring that all products are labelled according to recognized environmental standards.

Improving our environmental record on a continual basis.

End of Life Statement

3Com processes allow for the recovery, reclamation and safe disposal of all end-of-life electronic components.

Regulated Materials Statement

3Com products do not contain any hazardous or ozone-depleting material.

CONTENTS

ABOUT THIS GUIDE

Conventions 17
Related Documentation 17

1 CLI OVERVIEW

Introduction to the CLI 19
Command Level/Command View 19
CLI Features 29

2 LOGGING INTO AN ETHERNET SWITCH

Logging into an Ethernet Switch 33
Introduction to the User Interface 33

3 LOGGING IN THROUGH THE CONSOLE PORT

Introduction 35
Logging in through the Console Port 35
Console Port Login Configuration 37
Console Port Login Configuration with Authentication Mode Being None 39
Console Port Login Configuration with Authentication Mode Being Password 42
Console Port Login Configuration with Authentication Mode Being Scheme 46

4 LOGGING IN THROUGH TELNET

Introduction 51
Telnet Configuration with Authentication Mode Being None 52
Telnet Configuration with Authentication Mode Being Password 55
Telnet Configuration with Authentication Mode Being Scheme 58
Telneting to a Switch 62

5 LOGGING IN USING MODEM

Introduction 65
Configuration on the Administrator Side 65
Configuration on the Switch Side 65
Modem Connection Establishment 66
Modem Attributes Configuration 68

6 LOGGING IN THROUGH THE WEB-BASED NETWORK MANAGEMENT SYSTEM

Introduction 71
Establishing an HTTP Connection 71
Configuring the Login Banner 72
Enabling/Disabling the WEB Server 73

7 LOGGING IN THROUGH NMS

Introduction 75
Connection Establishment Using NMS 75

8 USER CONTROL

Introduction 77
Controlling Telnet Users 77
Controlling Network Management Users by Source IP Addresses 79
Controlling Web Users by Source IP Address 80

9 CONFIGURATION FILE MANAGEMENT

Introduction to Configuration File 83
Configuration File-Related Operations 83

10 VLAN OVERVIEW

VLAN Overview 87
Port-Based VLAN 89
Protocol-Based VLAN 91

11 VLAN CONFIGURATION

VLAN Configuration 95
Configuring a Port-Based VLAN 97
Configuring a Protocol-Based VLAN 100

12 VOICE VLAN CONFIGURATION

Voice VLAN Overview 105
Voice VLAN Configuration 108
Displaying and Maintaining Voice VLAN Configuration 110
Voice VLAN Configuration Example 110

13 ISOLATE-USER-VLAN CONFIGURATION

Isolate-User-VLAN Overview 113
Isolate-User-VLAN Configuration 114
Displaying Isolate-User-VLAN Configuration 116
Isolate-User-VLAN Configuration Example 116

14 SUPER VLAN

Super VLAN Overview 121
Super VLAN Configuration 121
Displaying Super VLAN 123
Super VLAN Configuration Example 124

15 IP ADDRESS CONFIGURATION

IP Address Overview 127
Configuring an IP Address for a VLAN Interface 129
Displaying IP Address Configuration 130
IP Address Configuration Example 130
Troubleshooting 130

16 IP PERFORMANCE CONFIGURATION

IP Performance Overview 131
IP Performance Configuration 131
Configuring TCP Attributes 132
Configuring to Send Special IP Packets to CPU 132
Enabling Forwarding of Directed Broadcasts to a Directly Connected Network 132
Disabling ICMP Error Message Sending 133
Displaying and Debugging IP Performance 133
Troubleshooting 134

17 IPX CONFIGURATION

IPX Protocol Overview 137
IPX Configuration 138
Displaying and Debugging IPX 145
IPX Configuration Example 145
Troubleshooting IPX 147

18 GVRP CONFIGURATION

Introduction to GARP and GVRP 153
GVRP Configuration 156
Displaying and Maintaining GVRP 157
GVRP Configuration Example 158

19 QINQ CONFIGURATION

QinQ Overview 159
QinQ Configuration 160
Displaying QinQ 161
QinQ Configuration Example 161

20 SELECTIVE QINQ CONFIGURATION

Selective QinQ Overview 165

Selective QinQ Configuration 165
Configuring Outer Tag Replacement 166
Selective QinQ Configuration Example 167

21 SHARED VLAN CONFIGURATION

Shared VLAN Overview 169
Shared VLAN Configuration 170
Displaying Shared VLAN 170
Shared VLAN Configuration Example 171

22 PORT BASIC CONFIGURATION

Ethernet Port Configuration 173
Ethernet Port Configuration Example 180
Troubleshooting Ethernet Port Configuration 181

23 LINK AGGREGATION CONFIGURATION

Overview 183
Link Aggregation Configuration 189
Displaying and Maintaining Link Aggregation Configuration 192
Link Aggregation Configuration Example 193

24 PORT ISOLATION CONFIGURATION

Port Isolation Overview 195
Configuring Port Isolation 195
Displaying Port Isolation Configuration 196
Port Isolation Configuration Example 196

25 PORT SECURITY CONFIGURATION

Port Security Overview 199
Port Security Configuration 202
Displaying Port Security Configuration 206
Port Security Configuration Example 206

26 PORT BINDING CONFIGURATION

Port Binding Overview 209
Displaying Port Binding Configuration 209
Port Binding Configuration Example 210

27 DLDP CONFIGURATION

Overview 211
DLDP Fundamentals 212
DLDP Configuration 218
DLDP Network Example 222

28 MAC Address Table Management

Overview 225
Configuring MAC Address Table Management 227
Displaying and Maintaining MAC Address Configuration 230
Configuration Example 231

29 Centralized MAC Address Authentication Configuration

Centralized MAC Address Authentication Overview 233
Centralized MAC Address Authentication Configuration 234
Displaying and Debugging Centralized MAC Address Authentication 237
Centralized MAC Address Authentication Configuration Example 237

30 MSTP Configuration

MSTP Overview 241
Root Bridge Configuration 246
Leaf Node Configuration 259
The mCheck Configuration 263
Protection Function Configuration 264
Digest Snooping Configuration 268
Rapid Transition Configuration 269
BPDU Tunnel Configuration 272
STP Maintenance Configuration 274
MSTP Displaying and Debugging 274
MSTP Implementation Example 275
BPDU Tunnel Configuration Example 277

31 IP Routing Protocol Overview

Introduction to IP Route and Routing Table 281
Routing Management Policy 283

32 Static Route Configuration

Introduction to Static Route 285
Static Route Configuration 286
Displaying and Maintaining the Routing Table 286
Static Route Configuration Example 287
Troubleshooting a Static Route 288

33 RIP Configuration

RIP Overview 289
Introduction to RIP Configuration Tasks 290
Basic RIP Configuration 291
RIP Route Control 293
RIP Network Adjustment and Optimization 296
Displaying and Maintaining RIP Configuration 298
RIP Configuration Example 299

Troubleshooting RIP Configuration 300

34 OSPF CONFIGURATION

OSPF Overview 301
Introduction to OSPF Configuration Tasks 307
Basic OSPF Configuration 309
OSPF Area Attribute Configuration 311
OSPF Network Type Configuration 312
OSPF Route Control 313
OSPF Network Adjustment and Optimization 316
Displaying OSPF Configuration 320
OSPF Configuration Example 321
Troubleshooting OSPF Configuration 325

35 IS-IS CONFIGURATION

IS-IS Overview 327
Introduction to IS-IS Configuration 332
IS-IS Basic Configuration 333
Displaying Integrated IS-IS Configuration 345
Integrated IS-IS Configuration Example 345

36 BGP CONFIGURATION

BGP Overview 349
BGP Configuration Tasks 354
Basic BGP Configuration 355
Configuring the Way to Advertise/Receive Routing Information 356
Configuring BGP Route Attributes 361
Adjusting and Optimizing a BGP Network 363
Configuring a Large-Scale BGP Network 365
Displaying and maintaining BGP 368
Configuration Example 369
BGP Error Configuration Example 376

37 IP ROUTING POLICY CONFIGURATION

IP Routing Policy Overview 377
IP Routing Policy Configuration 378
Displaying IP Routing Policy 383
IP Routing Policy Configuration Example 383
Troubleshooting IP Routing Policy 385

38 ROUTE CAPACITY CONFIGURATION

Route Capacity Configuration Overview 387
Route Capacity Configuration 387
Displaying Route Capacity Configuration 388

39 802.1x Configuration

Introduction to 802.1x 389
802.1x Configuration 399
Basic 802.1x Configuration 399
802.1x-Related Parameter Configuration 401
Advanced 802.1x Configuration 401
Displaying and Debugging 802.1x 403
Configuration Example 404

40 HABP Configuration

Introduction to HABP 409
HABP Server Configuration 409
HABP Client Configuration 410
Displaying HABP 410
HABP Configuration Example 410

41 Multicast Overview

Multicast Overview 413
Multicast Architecture 416
Forwarding Mechanism of Multicast Packets 420

42 GMRP Configuration

GMRP Overview 423
Configuring GMRP 423
Displaying and Maintaining GMRP 424
GMRP Configuration Example 424

43 IGMP Snooping Configuration

Overview 427
IGMP Snooping Configuration 430
Displaying and Maintaining IGMP Snooping 437
IGMP Snooping Configuration Example 438
Troubleshooting IGMP Snooping 440

44 Common Multicast Configuration

Overview 441
Common Multicast Configuration Tasks 441
Displaying Common Multicast Configuration 445

45 Static Multicast MAC Address Table Configuration

Overview 447
Configuring a Multicast MAC Address Entry 447
Displaying Multicast MAC Address 447

46 IGMP CONFIGURATION

Overview 449
IGMP Configuration Tasks 454
Displaying IGMP 460

47 PIM CONFIGURATION

PIM Overview 461
Common PIM Configuration 469
PIM-DM Configuration 472
PIM-SM Configuration 472
Displaying and Debugging PIM 475
PIM Configuration Examples 476
Troubleshooting PIM 479

48 MSDP CONFIGURATION

MSDP Overview 481
Configuring MSDP Basic Functions 487
Configuring Connection between MSDP Peers 488
Configuring SA Message Transmission 490
Displaying and Debugging MSDP Configuration 493
MSDP Configuration Example 494
Troubleshooting MSDP Configuration 504

49 AAA & RADIUS & HWTACACS CONFIGURATION

Overview 507
Configuration Tasks 516
AAA Configuration 518
RADIUS Configuration 525
HWTACACS Configuration 532
Displaying and Maintaining AAA & RADIUS & HWTACACS Information 536
AAA & RADIUS & HWTACACS Configuration Example 537
Troubleshooting AAA & RADIUS & HWTACACS Configuration 541

50 EAD CONFIGURATION

Introduction to EAD 543
Typical Network Application of EAD 543
EAD Configuration 544
EAD Configuration Example 545

51 TRAFFIC ACCOUNTING CONFIGURATION

Introduction to Traffic Accounting 547
Configuring Traffic Accounting 548
Displaying Traffic Accounting 549
Traffic Accounting Configuration Example 550

52 VRRP CONFIGURATION

VRRP Overview 553
VRRP Configuration 557
Displaying and Maintaining VRRP 559
VRRP Configuration Example 559
Troubleshooting VRRP 565

53 HA CONFIGURATION

HA Overview 567
HA Configuration 568
Displaying HA 569

54 ARP CONFIGURATION

Introduction to ARP 571
Configuring ARP 575
Displaying and Maintaining ARP Configuration 579
ARP Configuration Example 580

55 PROXY ARP CONFIGURATION

Proxy ARP Overview 583
Configuring Proxy ARP 584
Proxy ARP Configuration Example 584

56 DHCP OVERVIEW

Introduction to DHCP 589
DHCP IP Address Assignment 589
DHCP Packet Format 590
DHCP Packet Processing Modes 592
Protocols and Standards 592

57 DHCP SERVER CONFIGURATION

Introduction to DHCP Server 593
Global Address Pool-Based DHCP Server Configuration 594
Interface Address Pool-Based DHCP Server Configuration 600
DHCP Security Configuration 606
Displaying and Maintaining a DHCP Server 607
DHCP Server Configuration Example 607
Troubleshooting a DHCP Server 609

58 DHCP RELAY AGENT CONFIGURATION

Introduction to DHCP Relay Agent 611
Configuring DHCP Relay Agent 613
Displaying and Maintaining DHCP Relay Agent 620
DHCP Relay Agent Configuration Example 620

Troubleshooting DHCP Relay Agent 621

59 DHCP SNOOPING CONFIGURATION

Configuring DHCP Snooping 623
DHCP Snooping Configuration 628
Displaying and Maintaining DHCP Snooping 632
DHCP Snooping Configuration Example 632

60 ACL CONFIGURATION

ACL Overview 637
Choosing ACL Mode for Traffic Flows 639
Specifying the Matching Order of ACL Rules Sent to a Port 640
Configuring Time Ranges 640
Defining Basic ACLs 641
Defining Advanced ACLs 642
Defining Layer 2 ACLs 647
Defining User-Defined ACLs 649
Applying ACLs on Ports 650
Displaying ACL Configuration 652
ACL Configuration Example 653

61 QOS CONFIGURATION

Overview 657
QoS Supported by the Switch 7750 666
Setting Port Priority 666
Configuring Priority to Be Used When a Packet Enters an Output Queue 667
Configuring Priority Remark 669
Configuring Rate Limit on Ports 671
Configuring TP 672
Configuring Redirect 673
Configuring Queue-scheduling 674
Configuring Congestion Avoidance 675
Configuring Traffic Statistics 676
Configuring Assured Bandwidth 678
Configuring Bidirectional CAR 679
Configuring Traffic-Based Selective QinQ 679
QoS Configuration Example 681

62 MIRRORING CONFIGURATION

Overview 685
Mirroring Supported by the Switch 7750 688
Mirroring Configuration 688

63 CLUSTER

Cluster Overview 703

Management Device Configuration 708
Member Device Configuration 711
Intra-Cluster Configuration 713
Displaying and Maintaining a Cluster 713
Cluster Configuration Example 714

64 POE CONFIGURATION
PoE Overview 719
PoE Configuration 721
Displaying PoE Configuration 723
PoE Configuration Example 724

65 POE PSU SUPERVISION CONFIGURATION
Introduction to PoE PSU Supervision 727
AC Input Alarm Thresholds Configuration 727
DC Output Alarm Threshold Configuration 728
Displaying PoE Supervision Information 729
PoE PSU Supervision Configuration Example 729

66 POE PROFILE CONFIGURATION
Introduction to PoE Profile 731
PoE Profile Configuration Tasks 731
Displaying PoE Profile Configuration 732
PoE Profile Configuration Example 732

67 UDP-HELPER CONFIGURATION
Introduction to UDP-Helper 735
Configuring UDP-Helper 735
Displaying and Maintaining UDP-Helper 736
UDP-Helper Configuration Example 737

68 SNMP CONFIGURATION
SNMP Overview 739
Configuring SNMP Basic Functions 741
Configuring Trap 743
Displaying SNMP 744
SNMP Configuration Example 745

69 RMON CONFIGURATION
Introduction to RMON 747
RMON Configuration 749
Displaying RMON 750
RMON Configuration Example 750

70 NTP CONFIGURATION

Introduction to NTP 753
NTP Implementation Mode Configuration 757
Access Control Permission Configuration 759
NTP Authentication Configuration 759
Configuration of Optional NTP Parameters 761
Displaying and Debugging NTP 762
Configuration Example 762

71 SSH TERMINAL SERVICES

SSH Terminal Services 773
SFTP Service 784

72 FILE SYSTEM MANAGEMENT

File System Configuration 791

73 BIMS CONFIGURATION

Introduction to BIMS 797
BIMS Device Configuration Tasks 798
Basic Configuration of BIMS Device 798
Configuring BIMS Access Mode 799
BIMS Configuration Example 800

74 FTP AND TFTP CONFIGURATION

FTP Configuration 803
TFTP Configuration 810

75 INFORMATION CENTER

Information Center Overview 815
Information Center Configuration 819
Displaying and Debugging Information Center Configuration 825
Information Center Configuration Examples 825

76 DNS CONFIGURATION

DNS Overview 831
Configuring Static DNS Resolution 833
Configuring Dynamic DNS Resolution 833
Displaying and Maintaining DNS 834
Troubleshooting DNS Configuration 835

77 BOOTROM AND HOST SOFTWARE LOADING

Introduction to Loading Approaches 837
Local Software Loading 837

Remote Software Loading 846

78 BASIC SYSTEM CONFIGURATION & DEBUGGING

Basic System Configuration 853
Displaying the System Status 855
System Debugging 855

79 NETWORK CONNECTIVITY TEST

Network Connectivity Test 859

80 DEVICE MANAGEMENT

Introduction to Device Management 861
Device Management Configuration 861
Configuring Pause Frame Protection Mechanism 866
Configuring Layer 3 Connectivity Detection 867
Configuring Queue Traffic Monitoring 868
Configuring Error Packets Monitoring 868
Displaying the Device Management Configuration 869
Remote Switch Update Configuration Example 870

81 REMOTE-PING CONFIGURATION

Remote-ping Overview 873
Remote-ping Configuration 876
Remote-ping Configuration Example 889

82 RRPP CONFIGURATION

RRPP Overview 903
Master Node Configuration 909
Transit Node Configuration 911
Edge Node Configuration 912
Assistant Edge Node Configuration 914
Configuration Example 916

83 TELNET PROTECTION CONFIGURATION

Introduction 921
Telnet Protection Configuration 921

84 SMART LINK CONFIGURATION

Smart Link Overview 923
Configuring Smart Link 925
Displaying and Debugging Smart Link 928
Smart Link Configuration Example 928

85 MONITOR LINK CONFIGURATION

Introduction to Monitor Link 931
Configuring Monitor Link 932
Displaying Monitor Link Configuration 934
Monitor Link Configuration Example 934

86 CONFIGURING HARDWARE-DEPENDENT SOFTWARE

Configuring Boot ROM Upgrade with App File 937
Configuring Inter-Card Link State Adjustment 938
Configuring Internal Channel Monitoring 939
Configuring Switch Chip Auto-reset 939
Configuring CPU Usage Threshold 940

About This Guide

This guide describes the 3Com® Switch 7750 and how to install hardware, configure and boot software, and maintain software and hardware. This guide also provides troubleshooting and support information for your switch.

This guide is intended for Qualified Service personnel who are responsible for configuring, using, and managing the switches. It assumes a working knowledge of local area network (LAN) operations and familiarity with communication protocols that are used to interconnect LANs.

Always download the Release Notes for your product from the 3Com World Wide Web site and check for the latest updates to software and product documentation:

http://www.3com.com

Conventions

Table 1 lists icon conventions that are used throughout this guide.

Table 1 Notice Icons

Icon	Notice Type	Description
	Information note	Information that describes important features or instructions.
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device.
	Warning	Information that alerts you to potential personal injury.

Related Documentation

The following manuals offer additional information necessary for managing your Switch 7750:

- *Switch 7750 Command Reference Guide* — Provides detailed descriptions of command line interface (CLI) commands, that you require to manage your Switch 7750.
- *Switch 7750 Quick Reference Guide* — Provides a summary of command line interface (CLI) commands that are required for you to manage your Switch 7750.
- *Switch 7750 Getting Started Guide* — Provides detailed descriptions of the hardware, explains how to set up and install the hardware and software for you Switch 7750.

- *Switch 7750 Release Notes* — Contains the latest information about your product. If information in this guide differs from information in the release notes, use the information in the *Release Notes*.

These documents are available in Adobe Acrobat Reader Portable Document Format (PDF) on the CD-ROM that accompanies your router or on the 3Com World Wide Web site:

http://www.3com.com/

1 CLI OVERVIEW

Introduction to the CLI

A 3Com series Ethernet switch provides a command line interface (CLI) and commands for you to configure and manage the Ethernet switch. The CLI is featured by the following:

- Commands are grouped by levels. This prevents unauthorized users from operating the switch with relevant commands.
- Users can gain online help at any time by entering the question mark "?".
- Commonly used diagnosing utilities (such as Tracert and Ping) are available.
- Debugging information of various kinds is available.
- The command history is available. You can recall and execute a history command easily.
- You can execute a command by only entering part of the command in the CLI, as long as the keywords you input uniquely identify the corresponding ones.

Command Level/Command View

To prevent unauthorized accesses, commands are grouped by command levels.

Commands fall into four levels: visit, monitor, system, and manage:

- Visit level: Commands at this level are mainly used to diagnose network and change the language mode of user interface, and cannot be saved in configuration files. For example, the **ping**, **tracert**, and **language-mode** commands are at this level.
- Monitor level: Commands at this level are mainly used to maintain the system and diagnose service problems, and cannot be saved to configuration files. For example, the **display** and **debugging** commands are at this level.
- System level: Commands at this level are mainly used to configure services. Commands concerning routing and network layers are at this level. You can utilize network services by using these commands.
- Manage level: Commands at this level are associated with the basic operation of the system, and the system supporting modules. These commands provide supports to services. Commands concerning file system, FTP, TFTP, user management, and level setting are at this level.

Users logging into a switch also fall into four levels, each of which corresponding to one of the above command levels. Users at a specific level can only use the commands of the same level and those of the lower levels.

Switching between User Levels

A user can switch the user level from one to another by executing a related command after logging into a switch. The administrator can also set user level switching passwords as required.

Setting a user level switching password

Table 1 lists the operations to set a user level switching password.

Table 1 Set a user level switching password

Operation	Command	Description
Enter system view	**system-view**	-
Set a password for switching from a lower user level to the user level identified by the *level* argument	**super password** [**level** *level*] { **simple** | **cipher** } *password*	Optional A password is necessary only when a user switches from a lower user level to a higher user level.

Switching to another user level

Table 2 lists operations to switch to another user level.

Table 2 Switch to another user level

Operation	Command	Description
Switch to the user level identified by the *level* argument	**super** [*level*]	Required Execute this command in user view. If a password for switching to the user level identified by the *level* argument is set and you want to switch to a lower user level, you will remain at the lower user level unless you provide the correct password after executing this command.



- *If the user level is not specified when user level switching password are set or when user level is switched, the user level is 3 by default.*
- *For security purpose, the password a user enters when switching to a higher user level is not displayed. A user will remain at the original user level if the user has tried three times to enter the correct password but fails to do this.*

Configuring the Level of a Specific Command in a Specific View

You can configure the level of a specific command in a specific view. Commands fall into four command levels: visit, monitor, system, and manage, which are identified as 0, 1, 2, and 3 respectively. The administrator can change the command level a command belongs to.

Table 3 lists the operations to configure the level of a specific command.

Table 3 Configure the level of a specific command in a specific view

Operation	Command	Description
Enter system view	**system-view**	-

Table 3 Configure the level of a specific command in a specific view

Operation	Command	Description
Configure the level of a specific command in a specific view	**command-privilege level** *level* **view** *view command*	Required Use this command with caution to prevent inconvenience on maintenance and operation.

CLI Views

CLI views are designed for different configuration tasks. They are interrelated. You will enter user view once you log into a switch successfully, where you can perform operations such as displaying operation status and statistical information. In addition, by executing the **system-view** command, you can enter system view, where you can enter other views by executing the corresponding commands.

The following CLI views are provided:

- User view
- System view
- M-Ethernet interface view
- Ethernet port view
- Null interface view
- Tunnel interface view
- AUX interface view
- VLAN view
- VLAN interface view
- Loopback interface view
- Local user view
- User interface view
- FTP client view
- SFTP client view
- Cluster view
- DHCP address pool view
- MST region view
- RRPP domain view
- MSDP region view
- Port-isolate-group view
- HWping view
- Public key view
- Public key code view
- PIM view
- RIP view
- OSPF view
- OSPF area view

- BGP view
- BGP IPv4 family multicast view
- IS-IS view
- ES-IS view
- Routing policy view
- Basic ACL view
- Advanced ACL view
- Layer 2 ACL view
- User-defined ACL view
- Traffic-group view
- QoS view
- QinQ view
- RADIUS scheme view
- HWTACACS scheme view
- ISP domain view
- RprGE view
- PoE-profile view
- Traffic-accounting view
- Netstream autonomous system view
- Netstream protocol - port aggregation view
- Netstream source prefix aggregation view
- Netstream destination prefix aggregation view
- Netstream source and destination aggregation view
- Smart-link group view

Table 4 lists information about CLI views (including the operations you can performed in these views, how to enter these views, and so on).

Table 4 CLI views

View	Available operation	Prompt example	Enter method	Quit method
User view	Display operation status and statistical information	<SW7750>	Enter user view once logging into the switch.	Execute the **quit** command in user view to log out of the switch.
System view	Configure system parameters	[SW7750]	Execute the **system-view** command in user view.	Execute the **quit** or **return** command to return to user view.

Table 4 CLI views

View	Available operation	Prompt example	Enter method	Quit method
M-Ethernet interface view	Configure M-Ethernet interface parameters	[SW7750-M-Ethernet0/0/0]	Manage Ethernet port view. Execute the **interface m-ethernet** 0/0/0 command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
Ethernet port view	Configure Ethernet port parameters	[SW7750-Ethernet3/0/1]	100 M Ethernet port view Execute the **interface ethernet** 3/0/1 command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
		[SW7750-GigabitEthernet4/0/1]	Gigabit Ethernet port view Execute the **interface gigabitethernet** 4/0/1 command in system view.	
Null interface view	Configure null interface parameters	[SW7750-NULL0]	Execute the **interface null** 0 command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
Tunnel interface view	Configure tunnel interface parameters	[SW7750-Tunnel0]	Execute the **interface tunnel** 0 command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
AUX interface view	Configure AUX interface parameters	[SW7750-Aux0/0/0]	Execute the **interface aux** 0/0/0 command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
VLAN view	Configure VLAN parameters	[SW7750-vlan1]	Execute the **vlan** 1 command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
VLAN interface view	Configure IP interface parameters for VLANs	[SW7750-Vlan-interface1]	Execute the **interface vlan-interface** 1 command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.

Table 4 CLI views

View	Available operation	Prompt example	Enter method	Quit method
Loopback interface view	**Configure Loopback interface parameters**	[SW7750-LoopBack0]	Execute the **interface loopback** 0 command in system view	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
Local user view	Configure local user parameters	[SW7750-luser-user1]	Execute the **local-user** user1 command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
User interface view	Configure user interface parameters	[SW7750-ui0]	Execute the **user-interface** 0 command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
FTP client view	Configure FTP client parameters	[ftp]	Execute the **ftp** command in user view.	Execute the **quit** command to return to user view.
SFTP client view	Configure SFTP client parameters	<sftp-client>	Execute the **sftp** 10.1.1.1 command in system view.	Execute the **quit** command to return to user view.
Cluster view	Configure cluster parameters	[SW7750-cluster]	Execute the **cluster** command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
DHCP address pool view	Configure DHCP address pool parameters	[SW7750-dhcp-pool-1]	Execute the **dhcp server ip-pool** 1 command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
MST region view	Configure MST region parameters	[SW7750-mst-region]	Execute the **stp region-configuration** command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
RRPP domain view	Configure RRPP domain parameters	[SW7750-rrpp-domain1]	Execute the **rrpp domain** 1 command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.

Table 4 CLI views

View	Available operation	Prompt example	Enter method	Quit method
MSDP domain view	Configure MSDP domain parameters	[SW7750-msdp]	Execute the **msdp** command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
Port-isolate-group view	Configure port-isolate-group parameters	[SW7750-port-isolate-group1]	Execute the **port-isolate group** 1 command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
HWping view	Configure HWping test group parameters	[SW7750-nqa-administrator-test]	Execute the **nqa administrator test** command in system view	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
Public key view	Configure RSA public keys for secure shell (SSH) users	[SW7750-rsa-public-key]	Execute the **rsa peer-public-key** 3Com003 command in system view.	Execute the **peer-public-key end** command to return to system view.
Public key code view	Edit RSA public keys of SSH users	[SW7750-rsa-key-code]	Execute the **public-key-code begin** command in public key view.	Execute the **public-key-code end** command to return to public key view.
PIM view	Configure PIM parameters	[SW7750-pim]	Execute the **pim** command in system view. Use the **multicast routing-enable** command in system view to enable multicast routing if multicast routing is disabled.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
RIP view	Configure RIP parameters	[SW7750-rip]	Execute the **rip** command in system view	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
OSPF view	Configure OSPF protocol parameters	[SW7750-ospf-1]	Execute the **ospf** command in system view	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.

Table 4 CLI views

View	Available operation	Prompt example	Enter method	Quit method
OSPF area view	Configure OSPF area parameters	[SW7750-ospf-1 -area-0.0.0.1]	Execute the **area** 1 command in OSPF view	Execute the **quit** command to return to OSPF view. Execute the **return** command to return to user view.
BGP view	Configure parameters for the (border gateway protocol) BGP protocol	[SW7750-bgp]	Execute the **bgp** 100 command in system view	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
BGP IPv4 family multicast view	Configure parameters for BGP IPv4 family multicast	[SW7750-bgp-a f-mul]	Execute the **ipv4-family multicast** command in BGP view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
IS-IS view	Configure IS-IS parameters	[SW7750-isis]	Execute the **isis** command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
ES-IS view	Configure parameters for the ES-IS protocol	[SW7750-esis]	Execute the **esis** command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
Routing policy view	Configure routing policies	[SW7750-route-policy]	Execute the **route-policy** policy1 **permit node** 10 command in system view	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
Basic ACL view	Define rules for a basic ACL (ACLs with their IDs ranging from 2000 to 2999 are basic ACLs.)	[SW7750-acl-basic-2000]	Execute the **acl number** 2000 command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
Advanced ACL view	Define rules for an advanced ACL (ACLs with their IDs ranging from 3000 to 3999 are advanced ACLs.)	[SW7750-acl-adv-3000]	Execute the **acl number** 3000 command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.

Table 4 CLI views

View	Available operation	Prompt example	Enter method	Quit method
Layer 2 ACL view	Define the sub-rules of Layer 2 ACLs, which is numbered from 4,000 to 4,999.	[SW7750-acl-link-4000]	Execute the **acl number** 4000 command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
User-defined ACL view	Define the sub-rules of user-defined ACLs, which are in the range of 5000 to 5999	[SW7750-acl-user-5000]	Execute the **acl number** 5000 command in system view	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
Traffic-group view	Configure traffic group parameters	[SW7750-traffic-group-1]	Execute the **traffic-accounting traffic-group** 1 command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
QoS view	Configure QoS parameters	[SW7750-qoss-GigabitEthernet4/0/1] or: [SW7750-qosb-GigabitEthernet4/0/1]	Execute the **qos** command in Ethernet port view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
QinQ view	Create QinQ instances and configure parameters for QinQ	[SW7750-GigabitEthernet4/0/1-vid-1000]	Execute the **vlan-vpn vid** 1000 **uplink Ethernet** 1/0/5 **untagged** command in Ethernet port view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
RADIUS scheme view	Configure RADIUS parameters	[SW7750-radius-1]	Execute the **radius scheme** 1 command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
HWTACACS scheme view	Configure parameters for the HWTACACS protocol	[SW7750-hwtacacs-1]	Execute the **hwtacacs scheme** 1 command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
ISP domain view	Configure parameters for an ISP domain	[SW7750-isp-aabbcc.net]	Execute the **domain** aabbcc.net command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.

Table 4 CLI views

View	Available operation	Prompt example	Enter method	Quit method
RprGE view	Configure RprGE logical interface attributes	[SW7750-RprGE 1/0/1]	Execute the **interface** RprGE 1/0/1 command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
PoE profile view	Configure PoE profile parameters	[SW7750 -poe-profile-test]	Execute the **poe-profile** test command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
Traffic accounting view	Configure traffic accounting parameters	[SW7750 -accounting-slot -0]	Execute the **traffic-accounting accounting-slot** 0 command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
Netstream autonomous system aggregation view	Configure netstream autonomous system aggregation parameters	[SW7750 -aggregation-as]	Execute the **ip netstream aggregation as** command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
Netstream protocol -port aggregation view	Configure netstream protocol-port aggregation parameters	[SW7750 -aggregation-protport]	Execute the **ip netstream aggregation protocol-port** command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
Netstream source prefix aggregation view	Configure netstream source prefix aggregation parameters	[SW7750 -aggregation-srcpre]	Execute the **ip netstream aggregation source-prefix** command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
Netstream destination prefix aggregation view	Configure netstream destination aggregation parameters	[SW7750 -aggregation-dstpre]	Execute the **ip netstream aggregation destination-prefix** command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
Netstream source and destination aggregation view	Configure netstream source and destination aggregation parameters	[SW7750-aggregation-prefix]	Execute the **ip netstream aggregation prefix** command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.

Table 4 CLI views

View	Available operation	Prompt example	Enter method	Quit method
Smart-link group view	Configure smart-link group parameters	[SW7750-smlk-group1]	Execute the **smart-link group** command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.

CLI Features

Online Help

CLI provides two types of online help: complete online help and partial online help. They assist you with your configuration.

Complete online help

Enter a "?" character in any view on your terminal to display all the commands available in the view and their brief descriptions. The following takes user view as an example.

```
<SW7750> ?
User view commands:
  boot            Set boot option
  cd              Change current directory
  clock           Specify the system clock
  cluster         Run cluster command
  copy            Copy from one file to another
  debugging       Enable system debugging functions
  delete          Delete a file
  dir             List files on a file system
  display         Display current system information
  <omitted>
```

Enter a command, a space, and a "?" character (instead of a keyword available in this position of the command) on your terminal to display all the available keywords and their brief descriptions. The following takes the **clock** command as an example.

```
<SW7750> clock ?
  datetime      Specify the time and date
  summer-time   Configure summer time
  timezone      Configure time zone
```

Enter a command, a space, and a "?" character (instead of an argument available in this position of the command) on your terminal to display all the available arguments and their brief descriptions. The following takes the **interface vlan** command as an example.

```
[SW7750] interface vlan-interface ?
  <1-4094>  VLAN interface number
[SW7750] interface vlan-interface 1 ?
  <cr>
```

The string <cr> means no argument is available in the position occupied by the "?" character. You can execute the command without providing any other information.

Partial online help

Enter a string followed directly by a "?" character on your terminal to display all the commands beginning with the string. For example:

```
<SW7750>pi?
    ping
```

Enter a command, a space, and a string followed by a "?" character on your terminal to display all the keywords that belong to the command and begin with the string (if available). For example:

```
<SW7750> display ver?
    version
```

Enter the first several characters of a keyword in a command and then press <Tab>, the complete keyword will be displayed on the terminal screen if the input characters uniquely identify a keyword. If the input characters match more than one keywords, press the Tab key repeatedly and all the keyword that match the input characters will be displayed on the terminal screen.

You can use the **language-mode** command to translate the help into Chinese.

Terminal Display

CLI provides the following display feature:

- Display suspending. That is, the displaying of output information can be split when the screen is full and you can then perform the three operations listed in Table 5 as needed.

Table 5 Displaying-related operations

Operation	Function
Press <Ctrl + C>	Suspend displaying and executing.
Press the space key	Scroll the output information up by one page.
Press <Enter>	Scroll the output information up by one line.

Command History

CLI can store the latest executed commands as history commands so that users can recall and execute them again. By default, CLI can store 10 history commands for each user. Table 6 lists history command-related operations.

Table 6 Access history commands

Operation	Operation	Description
Display history commands	Execute the **display history-command** command	This command displays valid history commands.
Recall the previous history command	Press the up-arrow key or <Ctrl + P>	This operation recalls the previous history command (if available).
Recall the next history command	Pressing the down-arrow key or <Ctrl + N>	This operation recalls the next history command (if available).

As the Up and Down keys have different meanings in HyperTerminal running on Windows 9x, these two keys can be used to recall history commands only in terminals running Windows 3.x or Telnet running in Windows 3.x. You can press <Ctrl + P> or <Ctrl + N> in Windows 9x to achieve the same purpose.

Error Messages

If the command you enter passes the syntax check, it will be successfully executed; otherwise an error message will appear. Table 7 lists the common error messages.

Table 7 Common error messages

Error message	Description
Unrecognized command	The command does not exist.
	The keyword does not exist.
	The parameter type is wrong.
	The parameter value is out of range.
Incomplete command	The command entered is incomplete.
Too many parameters	You have entered too many parameters.
Ambiguous command	The parameters entered are ambiguous.
Wrong parameter	The input parameter is wrong

Command Edit

The CLI provides basic command edit functions and supports multi-line editing. The maximum number of characters a command can contain is 254. Table 8 lists the CLI edit operations.

Table 8 Edit operations

Press...	To...
A common key	Insert the character the key represents at the cursor and move the cursor one character to the right if the edit buffer is not full.
The Backspace key	Delete the character on the left of the cursor and move the cursor one character to the left.
The left arrow key or <Ctrl + B>	Move the cursor one character to the left.
The right arrow key or <Ctrl + F>	Move the cursor one character to the right.
The up arrow key or <Ctrl + P>	Access history commands.
The down arrow key or <Ctrl + N>	
The Tab key	Utilize the partial online help. That is, when you enter an incomplete keyword and the Tab key, if the input keyword uniquely identifies an existing keyword, the system completes the keyword and displays the command on the next line. If the input keyword matches more than one keyword, press the Tab key repeatedly, all the keywords are displayed on the terminal screen, with each keyword on a line. If the input keyword matches no keyword, the system displays your original input on a new line without any change.

2 LOGGING INTO AN ETHERNET SWITCH

Logging into an Ethernet Switch

You can log into a Switch 7750 Ethernet switch in one of the following ways:

- Logging in locally through the Console port
- Telneting locally or remotely to an Ethernet port
- Telneting to the Console port using a modem
- Logging in through NMS (network management station)

Introduction to the User Interface

Supported User Interfaces

Switch 7750 Ethernet switch supports two types of user interfaces: AUX and VTY.

Table 9 Description on user interface

User interface	Applicable user	Port used	Description
AUX	Users logging in through the Console port	Console port	Each switch can accommodate one AUX user.
VTY	Telnet users and SSH users	Ethernet port	Each switch can accommodate up to five VTY users.

The AUX port and the Console port of a 3Com switch are the same port. You will be in the AUX user interface if you log in through this port.

User Interface Number

Two kinds of user interface index exist: absolute user interface index and relative user interface index.

1. The absolute user interface indexes are as follows:
   - AUX user interface: 0
   - VTY user interfaces: Numbered after AUX user interfaces and increases in the step of 1
2. A relative user interface index can be obtained by appending a number to the identifier of a user interface type. It is generated by user interface type. The relative user interface indexes are as follows:
   - AUX user interface: AUX 0
   - VTY user interfaces: VTY 0, VTY 1, VTY 2, and so on.

Common User Interface Configuration

Table 10 Common user interface configuration

Operation	Command	Description
Lock the current user interface	**lock**	Optional Execute this command in user view. A user interface is not locked by default.
Specify to send messages to all user interfaces/a specified user interface	**send** { **all** | *number* | *type number* }	Optional Execute this command in user view.
Disconnect a specified user interface	**free user-interface** [*type*] *number*	Optional Execute this command in user view.
Enter system view	**system-view**	-
Enable copyright information displaying	**copyright-info enable**	Optional By default, copyright information displaying is disabled. That is, the copyright information is not displayed after a user logs into a switch successfully.
Enter user interface view	**user-interface** [*type*] *first-number* [*last-number*]	-
Set the command that is automatically executed when a user logs into the user interface	**auto-execute command** *text*	Optional By default, no command is automatically executed when a user logs into a user interface.
Display the information about the current user interface/all user interfaces	**display users** [**all**]	Optional These two commands can be executed in any view.
Display the physical attributes and configuration of the current/a specified user interface	**display user-interface** [*type number* | *number*]	

CAUTION:

- *The **auto-execute command** command may cause you unable to perform common configuration in the user interface, so use it with caution.*
- *Before executing the **auto-execute command** command and save your configuration, make sure you can log into the switch in other modes and cancel the configuration.*

3 LOGGING IN THROUGH THE CONSOLE PORT

Introduction

To log in through the Console port is the most common way to log into a switch. It is also the prerequisite to configure other login methods. Normally, you can log into a Switch 7750 Ethernet switch through its Console port.

To log into an Ethernet switch through its Console port, the communication configuration of the user terminal must be in accordance with that of the Console port.

Table 11 lists the default settings of a Console port.

Table 11 The default settings of a Console port

Setting	Default
Baud rate	9,600 bps
Flow control	None
Check mode (Parity)	None
Stop bits	1
Data bits	8

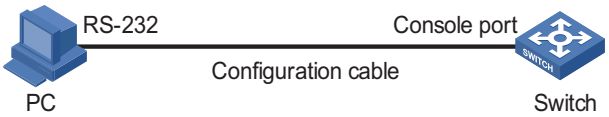
After logging into a switch, you can perform configuration for AUX users. Refer to "Console Port Login Configuration" on page 37 for more.

Logging in through the Console Port

Following are the procedures to connect to a switch through the Console port.

1 Connect the serial port of your PC/terminal to the Console port of the switch, as shown in Figure 1.

Figure 1 Diagram for setting the connection to the Console port



2 If you use a PC to connect to the Console port, launch a terminal emulation utility (such as Terminal in Windows 3.X or HyperTerminal in Windows 9X) and perform the configuration shown in Figure 2 through Figure 4 for the connection to be created. Normally, the parameters of a terminal are configured as those listed in Table 11. And the type of the terminal is set to VT100.

Figure 2 Create a connection

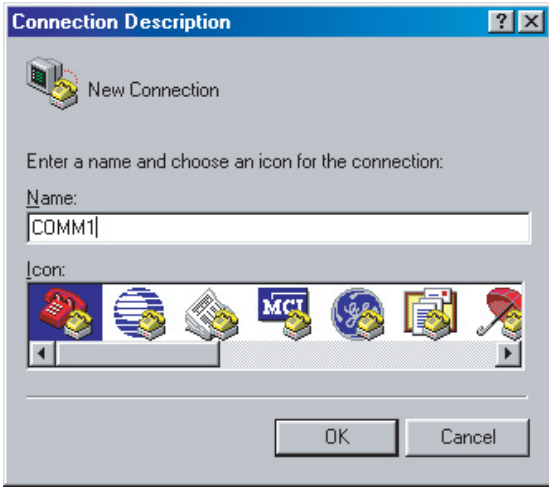
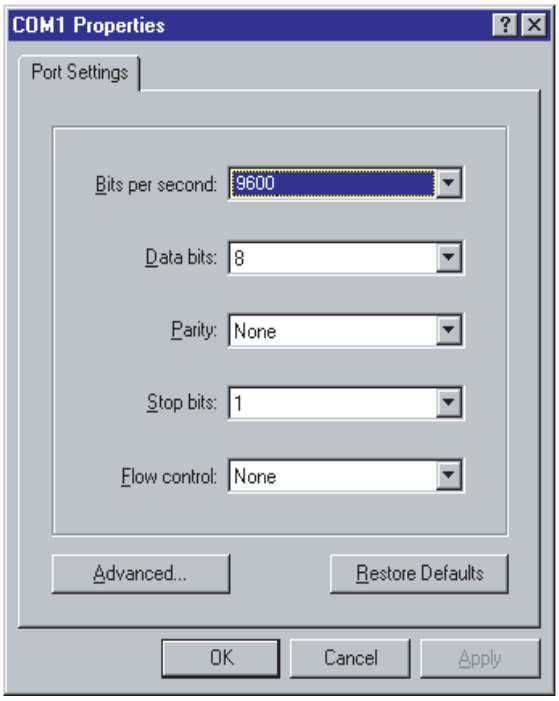


Figure 3 Specify the port used to establish the connection



Figure 4 Set port parameters



3 Turn on the switch. You will be prompted to press the Enter key if the switch successfully completes POST (power-on self test). The prompt (such as <SW7750>) appears after you press the Enter key.

4 You can then configure the switch or check the information about the switch by executing the corresponding commands. You can also acquire help by type the ? character. The commands available on a switch are described in the related module of the command manual.

Console Port Login Configuration

Common Configuration

Table 12 lists the common configuration of Console port login.

Table 12 Common configuration of Console port login

Configuration		Remarks
Console port configuration	Baud rate	Optional The default baud rate is 9,600 bps.
	Check mode	Optional By default, the check mode of the Console port is set to “none”, which means no check bit.
	Stop bits	Optional The default stop bits of a Console port is 1.
	Data bits	Optional The default data bits of a Console port is 8.

Table 12 Common configuration of Console port login

Configuration		Remarks
AUX user interface configuration	Configure the command level available to the users logging into the AUX user interface	Optional By default, commands of level 3 are available to the users logging into the AUX user interface.
Terminal configuration	Make terminal services available	Optional By default, terminal services are available in all user interfaces
	Set the maximum number of lines the screen can contain	Optional By default, the screen can contain up to 24 lines.
	Set history command buffer size	Optional By default, the history command buffer can contain up to 10 commands.
	Set the timeout time of a user interface	Optional The default timeout time is 10 minutes.



CAUTION: *Changing of Console port configuration terminates the connection to the Console port. To establish the connection again, you need to modify the configuration of the termination emulation utility running on your PC accordingly. Refer to "Logging in through the Console Port" on page 35 for more.*

Console Port Login Configurations for Different Authentication Modes

Table 13 lists Console port login configurations for different authentication modes.

Table 13 Console port login configurations for different authentication modes

Authentication mode	Console port login configuration		Remarks
None	Perform common configuration	Perform common configuration for Console port login	Optional Refer to "Common Configuration" on page 37 for more.
Password	Configure the password	Configure the password for local authentication	Required
	Perform common configuration	Perform common configuration for Console port login	Optional Refer to "Common Configuration" on page 37 for more.

Table 13 Console port login configurations for different authentication modes

Authentication mode	Console port login configuration		Remarks
Scheme	Specify to perform local authentication or RADIUS authentication	AAA configuration specifies whether to perform local authentication or RADIUS authentication	Optional Local authentication is performed by default. Refer to "Configuring RADIUS Authentication/Authorization Servers" on page 525 for more.
	Configure user name and password	Configure user names and passwords for local/RADIUS users	Required ■ The user name and password of a local user are configured on the switch. ■ The user name and password of a RADIUS user are configured on the RADIUS server. Refer to user manual of RADIUS server for more.
	Manage AUX users	Set service type for AUX users	Required
	Perform common configuration	Perform common configuration for Console port login	Optional Refer to "Common Configuration" on page 37 for more.



Changes of the authentication mode of Console port login will not take effect unless you quit the command-line interface and then enter it again.

Console Port Login Configuration with Authentication Mode Being None

Configuration Procedure

Table 14 Console port login configuration with the authentication mode being none

Operation	Command	Description
Enter system view	**system-view**	-
Enter AUX user interface view	**user-interface aux** 0	-
Configure not to authenticate users	**authentication-mode none**	Required By default, users logging in through the Console port are not authenticated.

Table 14 Console port login configuration with the authentication mode being none

Operation		Command	Description
Configure the Console port	Set the baud rate	**speed** speed-value	Optional The default baud rate of an AUX port (also the Console port) is 9,600 bps.
	Set the check mode	**parity** { **even** | **mark** | **none** | **odd** | **space** }	Optional By default, the check mode of a Console port is set to **none**, that is, no check bit.
	Set the flow control mode	**flow-control** { **hardware** | **none** | **software** }	Optional By default, a Console port does not perform flow control.
	Set the stop bits	**stopbits** { **1** | **1.5** | **2** }	Optional The stop bits of a Console port is 1.
	Set the data bits	**databits** { **7** | **8** }	Optional The default data bits of a Console port is 8.
Configure the command level available to users logging into the user interface		**user privilege level** *level*	Optional By default, commands of level 3 are available to users logging into the AUX user interface.
Make terminal services available		**shell**	Optional By default, terminal services are available in all user interfaces.
Set the maximum number of lines the screen can contain		**screen-length** *screen-length*	Optional By default, the screen can contain up to 24 lines. You can use the **screen-length** 0 command to disable the function to display information in pages.
Set the history command buffer size		**history-command max-size** *value*	Optional The default history command buffer size is 10. That is, a history command buffer can store up to 10 commands by default.

Table 14 Console port login configuration with the authentication mode being none

Operation	Command	Description
Set the timeout time for the user interface	**idle-timeout** *minutes* [*seconds*]	Optional The default timeout time of a user interface is 10 minutes. With the timeout time being 10 minutes, the connection to a user interface is terminated if no operation is performed in the user interface within 10 minutes. You can use the **idle-timeout** 0 command to disable the timeout function.

Note that the command level available to users logging into a switch through the None authentication mode depends on both the **authentication-mode none** command and the **user privilege level** *level* command, as listed in the following table.

Table 15 Determine the command level (A)

Scenario			
Authentication mode	**User type**	**Command**	**Command level**
None (**authentication-mode none**)	Users logging in through Console ports	The **user privilege level** *level* command not executed	Level 3
		The **user privilege level** *level* command already executed	Determined by the *level* argument

Configuration Example

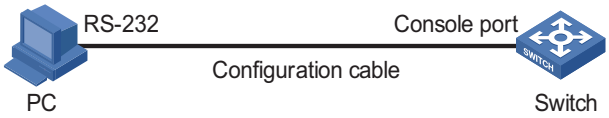
Network requirements

Perform the following configuration for users logging in through the Console port:

- Do not authenticate users logging in through the Console port.
- Commands of level 2 are available to users logging into the AUX user interface.
- The baud rate of the Console port is 19,200 bps.
- The screen can contain up to 30 lines.
- The history command buffer can contain up to 20 commands.
- The timeout time of the AUX user interface is 6 minutes.

Network diagram

Figure 5 Network diagram for AUX user interface configuration (with the authentication mode being none)



Configuration procedure

Enter system view.

```
<SW7750> system-view
```

Enter AUX user interface view.

```
[SW7750] user-interface aux 0
```

Specify not to authenticate users logging in through the Console port.

```
[SW7750-ui-aux0] authentication-mode none
```

Specify commands of level 2 are available to users logging into the AUX user interface.

```
[SW7750-ui-aux0] user privilege level 2
```

Set the baud rate of the Console port to 19,200 bps.

```
[SW7750-ui-aux0] speed 19200
```

Set the maximum number of lines the screen can contain to 30.

```
[SW7750-ui-aux0] screen-length 30
```

Set the maximum number of commands the history command buffer can store to 20.

```
[SW7750-ui-aux0] history-command max-size 20
```

Set the timeout time of the AUX user interface to 6 minutes.

```
[SW7750-ui-aux0] idle-timeout 6
```

Console Port Login Configuration with Authentication Mode Being Password

Configuration Procedure

Table 16 Console port login configuration with the authentication mode being password

Operation	Command	Description
Enter system view	**system-view**	-

Table 16 Console port login configuration with the authentication mode being password

Operation		Command	Description
Enter AUX user interface view		**user-interface aux** 0	-
Configure to authenticate users using the local password		**authentication-mode password**	Required By default, users logging into a switch through the Console port are not authenticated; while those logging in through Modems or Telnet are authenticated.
Set the local password		**set authentication password** { **cipher** | **simple** } *password*	Required
Configure the Console port	Set the baud rate	**speed** speed-value	Optional The default baud rate of an AUX port (also the Console port) is 9,600 bps.
	Set the check mode	**parity** { **even** | **mark** | **none** | **odd** | **space** }	Optional By default, the check mode of a Console port is set to **none**, that is, no check bit.
	Set the flow control mode	**flow-control** { **hardware** | **none** | **software** }	Optional By default, a Console port does not perform flow control.
	Set the stop bits	**stopbits** { **1** | **1.5** | **2** }	Optional The default stop bits of a Console port is 1.
	Set the data bits	**databits** { **7** | **8** }	Optional The default data bits of a Console port is 8.
Configure the command level available to users logging into the user interface		**user privilege level** *level*	Optional By default, commands of level 3 are available to users logging into the AUX user interface.
Make terminal services available to the user interface		**shell**	Optional By default, terminal services are available in all user interfaces.
Set the maximum number of lines the screen can contain		**screen-length** *screen-length*	Optional By default, the screen can contain up to 24 lines. You can use the **screen-length** 0 command to disable the function to display information in pages.
Set history command buffer size		**history-command max-size** *value*	Optional The default history command buffer size is 10. That is, a history command buffer can store up to 10 commands by default.

Table 16 Console port login configuration with the authentication mode being password

Operation	Command	Description
Set the timeout time for the user interface	**idle-timeout** *minutes* [*seconds*]	Optional The default timeout time of a user interface is 10 minutes. With the timeout time being 10 minutes, the connection to a user interface is terminated if no operation is performed in the user interface within 10 minutes. You can use the **idle-timeout** 0 command to disable the timeout function.

Note that the command level available to users logging into a switch through the password authentication mode depends on both the **authentication-mode password** and the **user privilege level** *level* command, as listed in the following table.

Table 17 Determine the command level (B)

Scenario		Command	
Authentication mode	**User type**		**Command level**
Local password authentication (**authentication-mode password**)	Users logging in through the AUX user interface	The **user privilege level** *level* command is not executed	Level 3
		The **user privilege level** *level* command is already executed	Determined by the *level* argument

Configuration Example

Network requirements

Perform the following configuration for users logging in through the Console port:

- Authenticate users logging in through the Console port using the local password.
- Set the local password to 123456 (in plain text).
- The commands of level 2 are available to users logging into the AUX user interface.
- The baud rate of the Console port is 19,200 bps.
- The screen can contain up to 30 lines.
- The history command buffer can store up to 20 commands.
- The timeout time of the AUX user interface is 6 minutes.

Network diagram

Figure 6 Network diagram for AUX user interface configuration (with the authentication mode being password)



Configuration procedure

Enter system view.

```
<SW7750> system-view
```

Enter AUX user interface view.

```
[SW7750] user-interface aux 0
```

Specify to authenticate users logging in through the Console port using the local password.

```
[SW7750-ui-aux0] authentication-mode password
```

Set the local password to 123456 (in plain text).

```
[SW7750-ui-aux0] set authentication password simple 123456
```

Specify commands of level 2 are available to users logging into the AUX user interface.

```
[SW7750-ui-aux0] user privilege level 2
```

Set the baud rate of the Console port to 19,200 bps.

```
[SW7750-ui-aux0] speed 19200
```

Set the maximum number of lines the screen can contain to 30.

```
[SW7750-ui-aux0] screen-length 30
```

Set the maximum number of commands the history command buffer can store to 20.

```
[SW7750-ui-aux0] history-command max-size 20
```

Set the timeout time of the AUX user interface to 6 minutes.

```
[SW7750-ui-aux0] idle-timeout 6
```

Console Port Login Configuration with Authentication Mode Being Scheme

Configuration Procedure

Table 18 Console port login configuration with the authentication mode being scheme

Operation		Command	Description
Enter system view		**system-view**	-
Configure the authentication mode	Enter the default ISP domain view	**domain** d*omain-name*	Optional By default, the local AAA scheme is applied. If you specify to apply the local AAA scheme, you need to perform the configuration concerning local user as well. If you specify to apply an existing scheme by providing the *radius-scheme-name* argument, you need to perform the following configuration as well: ■ Perform AAA&RADIUS configuration on the switch. (Refer to "AAA Configuration" on page 518 and "RADIUS Configuration" on page 525 for more.) ■ Configure the user name and password accordingly on the AAA server. (Refer to the user manual of AAA server.)
	Specify the AAA scheme to be applied to the domain	**scheme** { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] | **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] }	
	Quit to system view	**quit**	
Create a local user (Enter local user view.)		**local-user** *user-name*	Required No local user exists by default.
Set the authentication password for the local user		**password** { **simple** | **cipher** } *password*	Required
Specify the service type for AUX users		**service-type terminal** [**level** *level*]	Required
Quit to system view		**quit**	-
Enter AUX user interface view		**user-interface aux** 0	-

Table 18 Console port login configuration with the authentication mode being scheme

Operation		Command	Description
Configure to authenticate users locally or remotely		**authentication-mode scheme** [**command-authorization**]	Required The specified AAA scheme determines whether to authenticate users locally or remotely. Users are authenticated locally by default.
Configure the Console port	Set the baud rate	**speed** speed-value	Optional The default baud rate of the AUX port (also the Console port) is 9,600 bps.
	Set the check mode	**parity** { **even** | **mark** | **none** | **odd** | **space** }	Optional By default, the check mode of a Console port is set to **none**, that is, no check bit.
	Set the flow control mode	**flow-control** { **hardware** | **none** | **software** }	Optional By default, a Console port does not perform flow control.
	Set the stop bits	**stopbits** { **1** | **1.5** | **2** }	Optional The default stop bits of a Console port is 1.
	Set the data bits	**databits** { **7** | **8** }	Optional The default data bits of a Console port is 8.
Configure the command level available to users logging into the user interface		**user privilege level** *level*	Optional By default, commands of level 3 are available to users logging into the AUX user interface.
Make terminal services available to the user interface		**shell**	Optional By default, terminal services are available in all user interfaces.
Set the maximum number of lines the screen can contain		**screen-length** *screen-length*	Optional By default, the screen can contain up to 24 lines. You can use the **screen-length** 0 command to disable the function to display information in pages.

Table 18 Console port login configuration with the authentication mode being scheme

Operation	Command	Description
Set history command buffer size	**history-command max-size** *value*	Optional The default history command buffer size is 10. That is, a history command buffer can store up to 10 commands by default.
Set the timeout time for the user interface	**idle-timeout** *minutes* [*seconds*]	Optional The default timeout time of a user interface is 10 minutes. With the timeout time being 10 minutes, the connection to a user interface is terminated if no operation is performed in the user interface within 10 minutes. You can use the **idle-timeout** 0 command to disable the timeout function.

Note that the command level available to users logging into a switch through the scheme authentication mode depends on the **authentication-mode scheme** [**command-authentication**] command and the **service-type terminal** [**level** *level*] command, as listed in Table 19.

Table 19 Determine the command level

Scenario			
Authentication mode	**User type**	**Command**	**Command level**
authentication-mode scheme [**command-authorization**]	Users logging into the Console port and pass AAA&RADIUS or local authentication	The **service-type terminal** [**level** *level*] command is not configured.	Level 0 The default command level available for local users is level 0.
		The **service-type terminal** [**level** *level*] command is configured.	Determined by the *level* argument

Configuration Example

Network requirements

Perform the following configuration for users logging in through the Console port:

- Configure the name of the local user to be "guest".
- Set the authentication password of the local user to 1234567890 (in plain text).
- Set the service type of the local user to Terminal, the available command level of the user to 2.

- Configure to authenticate users logging in through the Console port in the scheme mode.
- The baud rate of the Console port is 19,200 bps.
- The screen can contain up to 30 lines.
- The history command buffer can store up to 20 commands.
- The timeout time of the AUX user interface is 6 minutes.

Network diagram

Figure 7 Network diagram for AUX user interface configuration (with the authentication mode being scheme)



Configuration procedure

Enter system view.

```
<SW7750> system-view
```

Create a local user named guest and enter local user view.

```
[SW7750] local-user guest
```

Set the authentication password to 1234567890 (in plain text).

```
[SW7750-luser-guest] password simple 1234567890
```

Set the service type of the local user to Terminal, with the available command level being 2.

```
[SW7750-luser-guest] service-type terminal level 2
[SW7750-luser-guest] quit
```

Enter AUX user interface view.

```
[SW7750] user-interface aux 0
```

Configure to authenticate users logging in through the Console port in the scheme mode.

```
[SW7750-ui-aux0] authentication-mode scheme
```

Set the baud rate of the Console port to 19,200 bps.

```
[SW7750-ui-aux0] speed 19200
```

Set the maximum number of lines the screen can contain to 30.

```
[SW7750-ui-aux0] screen-length 30
```

Set the maximum number of commands the history command buffer can store to 20.

```
[SW7750-ui-aux0] history-command max-size 20
```

Set the timeout time of the AUX user interface to 6 minutes.

```
[SW7750-ui-aux0] idle-timeout 6
```

4 LOGGING IN THROUGH TELNET

Introduction

You can manage and maintain a switch remotely by Telneting to the switch. To achieve this, you need to configure both the switch and the Telnet terminal accordingly.

Table 20 Requirements for Telnet to a switch

Item	Requirement
Switch	The IP address of the VLAN interface of the switch is configured and the route between the switch and the Telnet terminal is available. (Refer to "Configuring an IP Address for a VLAN Interface" on page 129 for more.)
	The authentication mode and other settings are configured. Refer to Table 21 and Table 22.
Telnet terminal	Telnet is running.
	The VLAN IP address of the switch is available.

Common Configuration

Table 21 lists the common Telnet configuration.

Table 21 Common Telnet configuration

Configuration		Description
VTY user interface configuration	Configure the command level available to users logging into the VTY user interface	Optional By default, commands of level 0 are available to users logging into a VTY user interface.
	Configure the protocols the user interface supports	Optional By default, Telnet and SSH protocol are supported.
VTY terminal configuration	Make terminal services available	Optional By default, terminal services are available in all user interfaces
	Set the maximum number of lines the screen can contain	Optional By default, the screen can contain up to 24 lines.
	Set history command buffer size	Optional By default, the history command buffer can contain up to 10 commands.
	Set the timeout time of a user interface	Optional The default timeout time is 10 minutes.
	Set whether to display the copyright statement information	Optional By default, the copyright information is displayed when a user logs into a switch through Telnet.

Telnet Configurations for Different Authentication Modes

Table 22 lists Telnet configurations for different authentication modes.

Table 22 Telnet configurations for different authentication modes

Authentication mode	Telnet configuration		Description
None	Perform common configuration	Perform common Telnet configuration	Optional Refer to Table 21.
Password	Configure the password	Configure the password for local authentication	Required
	Perform common configuration	Perform common Telnet configuration	Optional Refer to Table 21.
Scheme	Specify to perform local authentication or RADIUS authentication	AAA configuration specifies whether to perform local authentication or RADIUS authentication	Optional Local authentication is performed by default. Refer to "Configuring RADIUS Authentication/Authorization Servers" on page 525 for more.
	Configure user name and password	Configure user names and passwords for local/RADIUS users	Required ■ The user name and password of a local user are configured on the switch. ■ The user name and password of a remote user are configured on the RADIUS server. Refer to user manual of RADIUS server for more.
	Manage VTY users	Set service type for VTY users	Required
	Perform common configuration	Perform common Telnet configuration	Optional Refer to Table 21.

Telnet Configuration with Authentication Mode Being None

Configuration Procedure

Table 23 Telnet configuration with the authentication mode being none

Operation	Command	Description
Enter system view	**system-view**	-
Enter one or more VTY user interface views	**user-interface vty** *first-number* [*last-number*]	-
Configure not to authenticate users logging into VTY user interfaces	**authentication-mode none**	Required By default, VTY users are authenticated after logging in.

Table 23 Telnet configuration with the authentication mode being none

Operation	Command	Description
Configure the command level available to users logging into VTY user interface	**user privilege level** *level*	Optional By default, commands of level 0 are available to users logging into VTY user interfaces.
Configure the protocols to be supported by the VTY user interface	**protocol inbound** { **all** | **ssh** | **telnet** }	Optional By default, both Telnet protocol and SSH protocol are supported.
Make terminal services available	**shell**	Optional By default, terminal services are available in all user interfaces.
Set the maximum number of lines the screen can contain	**screen-length** *screen-length*	Optional By default, the screen can contain up to 24 lines. You can use the **screen-length** 0 command to disable the function to display information in pages.
Set the history command buffer size	**history-command max-size** *value*	Optional The default history command buffer size is 10. That is, a history command buffer can store up to 10 commands by default.
Set the timeout time of the VTY user interface	**idle-timeout** *minutes* [*seconds*]	Optional The default timeout time of a user interface is 10 minutes. With the timeout time being 10 minutes, the connection to a user interface is terminated if no operation is performed in the user interface within 10 minutes. You can use the **idle-timeout** 0 command to disable the timeout function.

Note that if you configure not to authenticate the users, the command level available to users logging into a switch depends on both the **authentication-mode none** command and the **user privilege level** *level* command, as listed in Table 24.

Table 24 Determine the command level when users logging into switches are not authenticated

Scenario			
Authentication mode	**User type**	**Command**	**Command level**
None (**authentication-mode none**)	VTY users	The **user privilege level** *level* command is not executed	Level 0
		The **user privilege level** *level* command is already executed	Determined by the *level* argument

Configuration Example

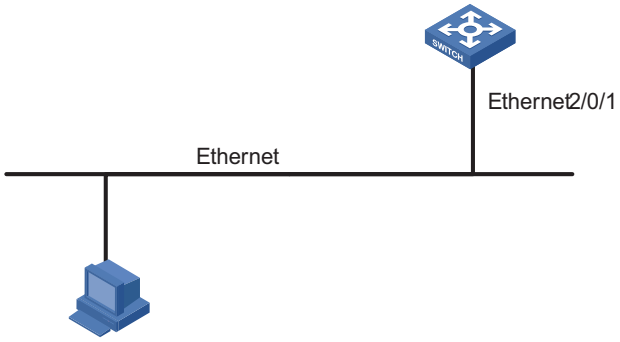
Network requirements

Perform the following configuration for Telnet users logging into VTY 0:

- Do not authenticate users logging into VTY 0.
- Commands of level 2 are available to users logging into VTY 0.
- VTY 0 user interface supports Telnet protocol.
- The screen can contain up to 30 lines.
- The history command buffer can contain up to 20 commands.
- The timeout time of VTY 0 is 6 minutes.

Network diagram

Figure 8 Network diagram for Telnet configuration (with the authentication mode being none)



Configuration procedure

Enter system view.

```
<SW7750> system-view
```

Enter VTY 0 user interface view.

```
[SW7750] user-interface vty 0
```

Configure not to authenticate Telnet users logging into VTY 0.

```
[SW7750-ui-vty0] authentication-mode none
```

Specify commands of level 2 are available to users logging into VTY 0.

```
[SW7750-ui-vty0] user privilege level 2
```

Configure Telnet protocol is supported.

```
[SW7750-ui-vty0] protocol inbound telnet
```

Set the maximum number of lines the screen can contain to 30.

```
[SW7750-ui-vty0] screen-length 30
```

Set the maximum number of commands the history command buffer can store to 20.

```
[SW7750-ui-vty0] history-command max-size 20
```

Set the timeout time to 6 minutes.

```
[SW7750-ui-vty0] idle-timeout 6
```

Telnet Configuration with Authentication Mode Being Password

Configuration Procedure

Table 25 Telnet configuration with the authentication mode being password

Operation	Command	Description
Enter system view	**system-view**	-
Enter one or more VTY user interface views	**user-interface vty** *first-number* [*last-number*]	-
Configure to authenticate users logging into VTY user interfaces using the local password	**authentication-mode password**	Required
Set the local password	**set authentication password** { **cipher** | **simple** } *password*	Required
Configure the command level available to users logging into the user interface	**user privilege level** *level*	Optional By default, commands of level 0 are available to users logging into VTY user interface.
Configure the protocol to be supported by the user interface	**protocol inbound** { **all** | **ssh** | **telnet** }	Optional By default, both Telnet protocol and SSH protocol are supported.
Make terminal services available	**shell**	Optional By default, terminal services are available in all user interfaces.

Table 25 Telnet configuration with the authentication mode being password

Operation	Command	Description
Set the maximum number of lines the screen can contain	**screen-length** *screen-length*	Optional By default, the screen can contain up to 24 lines. You can use the **screen-length** 0 command to disable the function to display information in pages.
Set the history command buffer size	**history-command max-size** *value*	Optional The default history command buffer size is 10. That is, a history command buffer can store up to 10 commands by default.
Set the timeout time of the user interface	**idle-timeout** *minutes* [*seconds*]	Optional The default timeout time of a user interface is 10 minutes. With the timeout time being 10 minutes, the connection to a user interface is terminated if no operation is performed in the user interface within 10 minutes. You can use the **idle-timeout** 0 command to disable the timeout function.

Note that if you configure to authenticate the users in the password mode, the command level available to users logging into a switch depends on both the **authentication-mode password** command and the **user privilege level** *level* command, as listed in Table 26.

Table 26 Determine the command level when users logging into switches are authenticated in the password mode

Scenario			
Authentication mode	**User type**	**Command**	**Command level**
Password (**authentication-mode password**)	VTY users	The **user privilege level** *level* command not executed	Level 0
		The **user privilege level** *level* command already executed	Determined by the *level* argument

Configuration Example

Network requirements

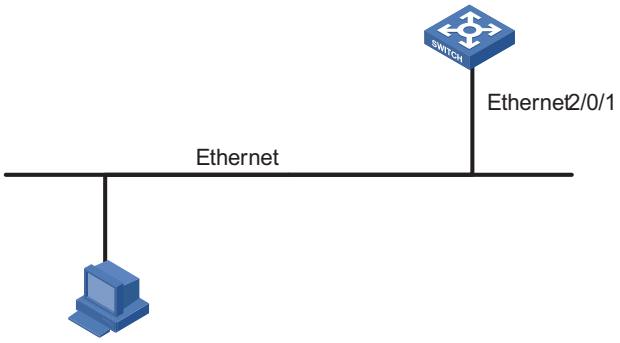
Assume that you are a level 3 AUX user and want to perform the following configuration for Telnet users logging into VTY 0:

- Authenticate users logging into VTY 0 using the local password.
- Set the local password to 123456 (in plain text).
- Commands of level 2 are available to users logging into VTY 0.

- Telnet protocol is supported.
- The screen can contain up to 30 lines.
- The history command buffer can contain up to 20 commands.
- The timeout time of VTY 0 is 6 minutes.

Network diagram

Figure 9 Network diagram for Telnet configuration (with the authentication mode being password)



Configuration procedure

Enter system view.

```
<SW7750> system-view
```

Enter VTY 0 user interface view.

```
[SW7750] user-interface vty 0
```

Configure to authenticate users logging into VTY 0 using the local password.

```
[SW7750-ui-vty0] authentication-mode password
```

Set the local password to 123456 (in plain text).

```
[SW7750-ui-vty0] set authentication password simple 123456
```

Specify commands of level 2 are available to users logging into VTY 0.

```
[SW7750-ui-vty0] user privilege level 2
```

Configure Telnet protocol is supported.

```
[SW7750-ui-vty0] protocol inbound telnet
```

Set the maximum number of lines the screen can contain to 30.

```
[SW7750-ui-vty0] screen-length 30
```

Set the maximum number of commands the history command buffer can store to 20.

```
[SW7750-ui-vty0] history-command max-size 20
```

Set the timeout time to 6 minutes.

```
[SW7750-ui-vty0] idle-timeout 6
```

Telnet Configuration with Authentication Mode Being Scheme

Configuration Procedure

Table 27 Telnet configuration with the authentication mode being scheme

Operation		Command	Description
Enter system view		**system-view**	-
Configure the authentication scheme	Enter the default ISP domain view	**domain** *domain-name*	Optional By default, the local AAA scheme is applied. If you specify to apply the local AAA scheme, you need to perform the configuration concerning local user as well. If you specify to apply an existing scheme by providing the *radius-scheme-name* argument, you need to perform the following configuration as well: ■ Perform AAA&RADIUS configuration on the switch. (Refer to "AAA Configuration" on page 518 and "RADIUS Configuration" on page 525 for more.) ■ Configure the user name and password accordingly on the AAA server. (Refer to the user manual of AAA server.)
	Configure the AAA scheme to be applied to the domain	**scheme** { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] | **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] }	
	Quit to system view	**quit**	
Create a local user and enter local user view		**local-user** *user-name*	Required No local user exists by default.
Set the authentication password for the local user		**password** { **simple** | **cipher** } *password*	Required
Specify the service type for VTY users		**service-type telnet** [**level** *level*]	Required
Quit to system view		**quit**	-
Enter one or more VTY user interface views		**user-interface vty** *first-number* [*last-number*]	-
Configure to authenticate users locally or remotely		**authentication-mode scheme** [**command-authorization**]	Required The specified AAA scheme determines whether to authenticate users locally or remotely. Users are authenticated locally by default.
Configure the command level available to users logging into the user interface		**user privilege level** *level*	Optional By default, commands of level 0 are available to users logging into the VTY user interfaces.

Table 27 Telnet configuration with the authentication mode being scheme

Operation	Command	Description
Configure the supported protocol	**protocol inbound** { **all** | **ssh** | **telnet** }	Optional Both Telnet protocol and SSH protocol are supported by default.
Make terminal services available	**shell**	Optional Terminal services are available in all use interfaces by default.
Set the maximum number of lines the screen can contain	**screen-length** *screen-length*	Optional By default, the screen can contain up to 24 lines. You can use the **screen-length** 0 command to disable the function to display information in pages.
Set history command buffer size	**history-command max-size** *value*	Optional The default history command buffer size is 10. That is, a history command buffer can store up to 10 commands by default.
Set the timeout time for the user interface	**idle-timeout** *minutes* [*seconds*]	Optional The default timeout time of a user interface is 10 minutes. With the timeout time being 10 minutes, the connection to a user interface is terminated if no operation is performed in the user interface within 10 minutes. You can use the **idle-timeout** 0 command to disable the timeout function.

Note that if you configure to authenticate the users in the scheme mode, the command level available to users logging into a switch depends on the **authentication-mode scheme** [**command-authentication**] command, the **user privilege level** *level* command, and the **service-type** | **telnet** [**level** *level*] command, as listed in Table 28.

Table 28 Determine the command level when users logging into switches are authenticated in the scheme mode

Scenario			
Authentication mode	**User type**	**Command**	**Command level**
Scheme (**authentication-mode scheme**) [**command-authorization**]	VTY users that are AAA&RADIUS authenticated or locally authenticated	The **user privilege level** *level* command is not executed, and the **service-type** command does not specify the available command level.	Level 0
		The **user privilege level** *level* command is not executed, and the **service-type** command specifies the available command level.	Determined by the **service-type** command
		The **user privilege level** *level* command is executed, and the **service-type** command does not specify the available command level.	Level 0
		The **user privilege level** *level* command is executed, and the **service-type** command specifies the available command level.	Determined by the **service-type** command
	VTY users that are authenticated in the RSA mode of SSH	The **user privilege level** *level* command is not executed, and the **service-type** command does not specify the available command level.	Level 0
		The **user privilege level** *level* command is not executed, and the **service-type** command specifies the available command level.	
		The **user privilege level** *level* command is executed, and the **service-type** command does not specify the available command level.	Determined by the **user privilege level** *level* command
		The **user privilege level** *level* command is executed, and the **service-type** command specifies the available command level.	
	VTY users that are authenticated in the password mode of SSH	The **user privilege level** *level* command is not executed, and the **service-type** command does not specify the available command level.	Level 0
		The **user privilege level** *level* command is not executed, and the **service-type** command specifies the available command level.	Determined by the **service-type** command
		The **user privilege level** *level* command is executed, and the **service-type** command does not specify the available command level.	Level 0
		The **user privilege level** *level* command is executed, and the **service-type** command specifies the available command level.	Determined by the **service-type** command



Refer to "AAA & RADIUS & HWTACACS Configuration Example" on page 537 and "SSH Terminal Services" on page 773.

Configuration Example

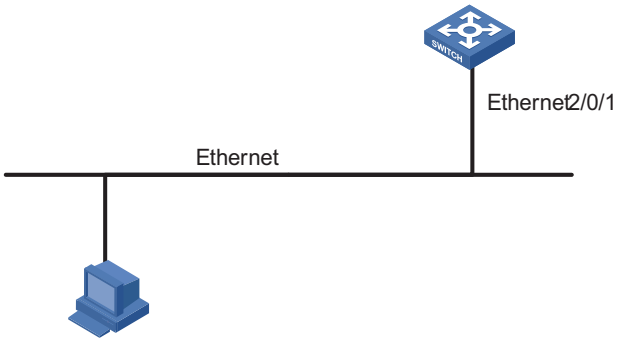
Network requirements

Perform the following configuration for Telnet users logging into VTY 0:

- Configure the name of the local user to be "guest".
- Set the authentication password of the local user to 1234567890 (in plain text).
- Set the service type of VTY users to Telnet, and the available command level to 2.
- Configure to authenticate users logging into VTY 0 in scheme mode.
- Only Telnet protocol is supported in VTY 0.
- The screen can contain up to 30 lines.
- The history command buffer can store up to 20 commands.
- The timeout time of VTY 0 is 6 minutes.

Network diagram

Figure 10 Network diagram for Telnet configuration (with the authentication mode being scheme)



Configuration procedure

Enter system view.

```
<SW7750> system-view
```

Create a local user named "guest" and enter local user view.

```
[SW7750] local-user guest
```

Set the authentication password of the local user to 1234567890 (in plain text).

```
[SW7750-luser-guest] password simple 1234567890
```

Set the service type to Telnet, with the available command level being 2.

```
[SW7750-luser-guest] service-type telnet level 2
```

Enter VTY 0 user interface view.

```
[SW7750] user-interface vty 0
```

Configure to authenticate users logging into VTY 0 in the scheme mode.

```
[SW7750-ui-vty0] authentication-mode scheme
```

Configure Telnet protocol is supported.

```
[SW7750-ui-vty0] protocol inbound telnet
```

Set the maximum number of lines the screen can contain to 30.

```
[SW7750-ui-vty0] screen-length 30
```

Set the maximum number of commands the history command buffer can store to 20.

```
[SW7750-ui-vty0] history-command max-size 20
```

Set the timeout time to 6 minutes.

```
[SW7750-ui-vty0] idle-timeout 6
```

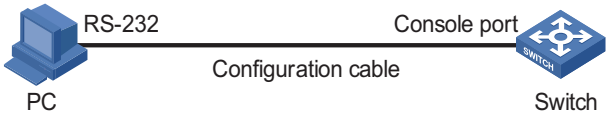
Telneting to a Switch

Telneting to a Switch from a Terminal

1 Assign an IP address to the interface of the VLAN of a switch. This can be achieved by executing the **ip address** command in VLAN interface view after you log in through the Console port.

- Connect the serial port of your PC/terminal to the Console port of the switch, as shown in Figure 11

Figure 11 Diagram for establishing connection to a Console port



- Launch a terminal emulation utility (such as Terminal in Windows 3.X or HyperTerminal in Windows 9X) on the PC, with the baud rate set to 9,600 bps, data bits set to 8, parity check set to none, and flow control set to none.
- Turn on the switch and press Enter as prompted. The prompt (such as <SW7750>) appears.
- Perform the following operations in the terminal window to assign an IP address to the VLAN interface of the switch.

Enter system view

```
<SW7750> system-view
```

Enter VLAN interface view.

```
[SW7750] interface Vlan-interface 1
```

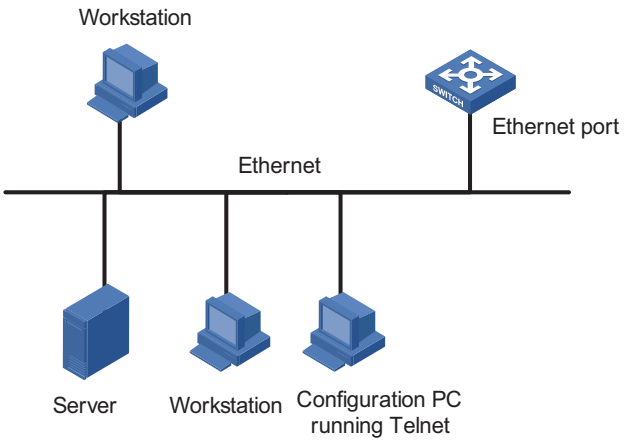
Set the IP address of the VLAN interface to 202.38.160.92, with the mask set 255.255.255.0.

```
[SW7750-Vlan-interface1] ip address 202.38.160.92 255.255.255.0
```

2 Perform Telnet-related configuration on the switch. Refer to "Telnet Configuration with Authentication Mode Being None" on page 52, "Telnet Configuration with Authentication Mode Being Password" on page 55, and "Telnet Configuration with Authentication Mode Being Scheme" on page 58 for more.

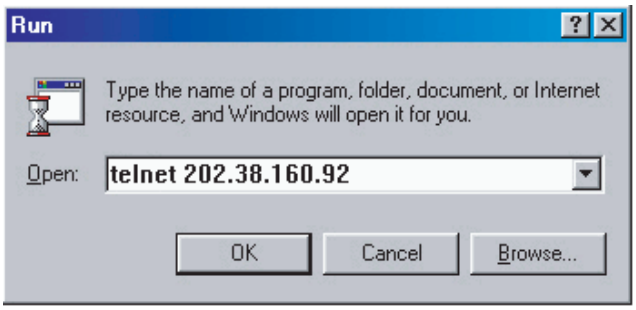
3 Connect your PC/terminal and the Switch to an Ethernet, as shown in Figure 12. Make sure the port through which the switch is connected to the Ethernet belongs to the VLAN and the route between your PC and the VLAN interface is reachable.

Figure 12 Network diagram for Telnet connection establishment



4 Launch Telnet on your PC, with the IP address of the VLAN interface of the switch as the parameter, as shown in Figure 13.

Figure 13 Launch Telnet



5 Enter the password when the Telnet window displays "Login authentication" and prompts for login password. The CLI prompt (such as <SW7750>) appears if the password is correct. If all VTY user interfaces of the switch are in use, you will fail to establish the connection and receive the message that says "All user interfaces are used, please try later!". A 3Com series Ethernet switch can accommodate up to five Telnet connections at same time.

6 After successfully Telneting to a switch, you can configure the switch or display the information about the switch by executing corresponding commands. You can also type ? at any time for help. For configuration commands, refer to the related modules in the command manual.

A Telnet connection is terminated if you delete or modify the IP address of the VLAN interface in the Telnet session.

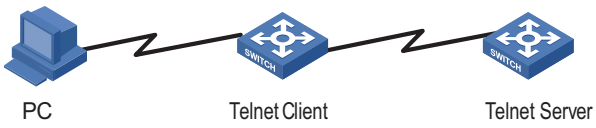
By default, commands of level 0 are available to Telnet users authenticated by password. Refer to "Command Level/Command View" on page 19 for information about command hierarchy.

Telneting to another Switch from the Current Switch

You can Telnet to another switch from the current switch. In this case, the current switch operates as the client, and the other operates as the server. If the interconnected Ethernet ports of the two switches are in the same LAN segment, make sure the IP addresses of the two management VLAN interfaces to which the two Ethernet ports belong to are of the same network segment, or the route between the two VLAN interfaces is available.

As shown in Figure 14, after Telneting to a switch (labeled as Telnet client), you can Telnet to another switch (labeled as Telnet server) by executing the **telnet** command and then to configure the later.

Figure 14 Network diagram for Telneting to another switch from the current switch



1. Perform Telnet-related configuration on the switch operating as the Telnet server. Refer to "Telnet Configuration with Authentication Mode Being None" on page 52, "Telnet Configuration with Authentication Mode Being Password" on page 55, and "Telnet Configuration with Authentication Mode Being Scheme" on page 58 for more.
2. Telnet to the switch operating as the Telnet client.
3. Execute the following command on the switch operating as the Telnet client:

   ```
   <SW7750> telnet xxxx
   ```

   Where xxxx is the IP address or the host name of the switch operating as the Telnet server. You can use the **ip host** to assign a host name to a switch.

4. Enter the password. If the password is correct, the CLI prompt (such as <SW7750>) appears. If all VTY user interfaces of the switch are in use, you will fail to establish the connection and receive the message that says "All user interfaces are used, please try later!".
5. Step 5: After successfully Telneting to the switch, you can configure the switch or display the information about the switch by executing corresponding commands. You can also type ? at any time for help. For detailed configuration commands, refer to the related modules in the command manual.

5 LOGGING IN USING MODEM

Introduction

The administrator can log into the Console port of a remote switch using a modem through PSTN (public switched telephone network) if the remote switch is connected to the PSTN through a modem to configure and maintain the switch remotely. When a network operates improperly or is inaccessible, you can log into the switches in the network in this way to configure these switches, to query logs and warning messages, and to locate problems.

To log into a switch in this way, you need to configure the administrator side and the switch properly, as listed in the following table.

Table 29 Requirements for logging into a switch using a modem

Item	Requirement
Administrator side	The PC can communicate with the modem connected to it.
	The modem is properly connected to PSTN.
	The telephone number of the switch side is available.
Switch side	The modem is connected to the Console port of the switch properly.
	The modem is properly configured.
	The modem is properly connected to PSTN and a telephone set.
	The authentication mode and other related settings are configured on the switch. Refer to Table 13.

Configuration on the Administrator Side

The PC can communicate with the modem connected to it. The modem is properly connected to PSTN. And the telephone number of the switch side is available.

Configuration on the Switch Side

Modem Configuration

Perform the following configuration on the modem directly connected to the switch:

```
AT&F        ---------------------- Restore the factory settings
ATS0=1  ---------------------- Configure to answer automatically af
ter the first ring
AT&D        ---------------------- Ignore DTR signal
AT&K0       ---------------------- Disable flow control
AT&R1       ---------------------- Ignore RTS signal
AT&S0       ---------------------- Set DSR to high level by force
ATEQ1&W ---------------------- Disable the modem from returning com
mand response and the result, save the changes
```

You can verify your configuration by executing the **AT&V** command.

The above configuration is unnecessary to the modem on the administrator side.

The configuration commands and the output of different modems may differ. Refer to the user manual of the modem when performing the above configuration.

Switch Configuration

After logging into a switch through its Console port by using a modem, you will enter the AUX user interface. Note the following when you perform the corresponding configuration on the switch

- *When you log in through the Console port using a modem, the baud rate of the Console port is usually set to a value lower than the transmission speed of the modem. Otherwise, packets may get lost.*
- *Other settings of the Console port, such as the check mode, the stop bits, and the data bits, remain the default.*

The configuration on the switch depends on the authentication mode the user is in. Refer to Table 13 for the information about authentication mode configuration.

Configuration on switch when the authentication mode is none

Refer to "Console Port Login Configuration with Authentication Mode Being None" on page 39.

Configuration on switch when the authentication mode is password

Refer to "Console Port Login Configuration with Authentication Mode Being Password" on page 42.

Configuration on switch when the authentication mode is scheme

Refer to "Console Port Login Configuration with Authentication Mode Being Scheme" on page 46.

Modem Connection Establishment

1. Before using Modem to log in to the switch, perform corresponding configuration for different authentication modes on the switch. Refer to "Console Port Login Configuration with Authentication Mode Being None" on page 39, "Console Port Login Configuration with Authentication Mode Being Password" on page 42, and "Console Port Login Configuration with Authentication Mode Being Scheme" on page 46 for more information.
2. Perform the following configuration to the modem directly connected to the switch.

```
AT&F       ---------------------- Restore the factory settings
ATS0=1  ---------------------- Configure to answer automatically af
ter the first ring
AT&D        ---------------------- Ignore DTR signal
AT&K0       ---------------------- Disable flow control
AT&R1       ---------------------- Ignore RTS signal
```

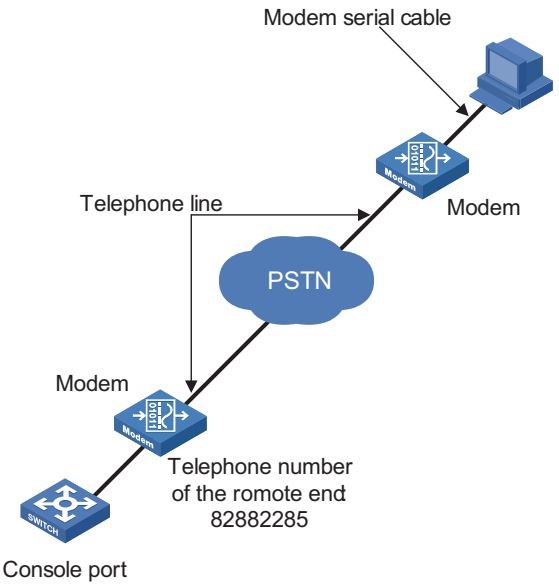
```
AT&S0       ----------------------- Set DSR to high level by force
ATEQ1&W ----------------------- Disable the modem from returning com
mand response and the result, save the changes
```

You can verify your configuration by executing the **AT&V** command.

- *The configuration commands and the output of different modems may differ. Refer to the user manual of the modem when performing the above configuration.*
- *It is recommended that the baud rate of the AUX port (also the Console port) be set to a value lower than the transmission speed of the modem. Otherwise, packets may get lost.*

3 Connect your PC, the modems, and the switch, as shown in the following figure.

Figure 15 Establish the connection by using modems



4 Launch a terminal emulation utility on the PC and set the telephone number to call the modem directly connected to the switch, as shown in Figure 16 and Figure 17. Note that you need to set the telephone number to that of the modem directly connected to the switch.

Figure 16 Set the telephone number

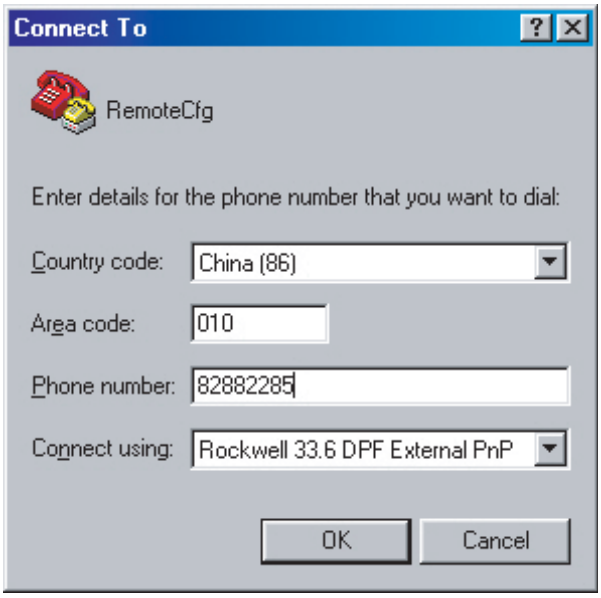
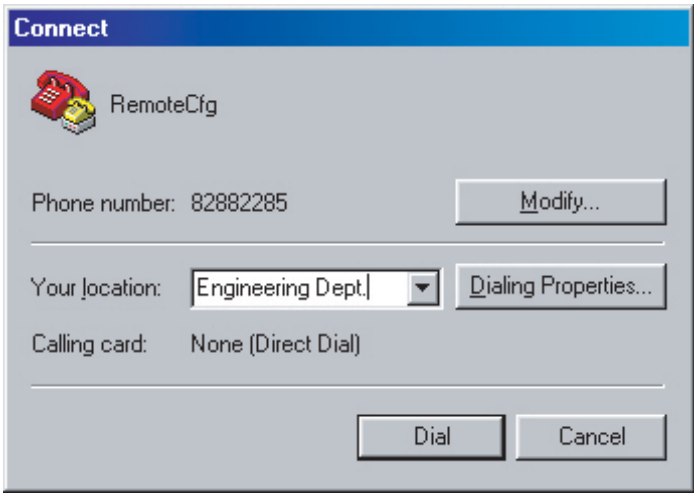


Figure 17 Call the modem



5 Provide the password when prompted. If the password is correct, the prompt (such as <SW7750>) appears. You can then configure or manage the switch. You can also enter the character ? at anytime for help. Refer to the related modules in the command manual for detailed configuration commands.

If you perform no AUX user-related configuration on the switch, the commands of level 3 are available to modem users. Refer to "Command Level/Command View" on page 19 for information about command level.

Modem Attributes Configuration

You can configure the Modem-related parameters.

Configuration Prerequisites

- You have configured the login mode for users on the switch.
- Network connection for Modem dial-up configuration has been established.

Configuration Procedure

Table 30 Configuration procedures of the Modem attribute

Operation	Command	Description
Enter system view	**system-view**	-
Enter AUX user interface view	**user-interface aux** 0	-
Enable Modem call-in/call-in and call-out	**modem** [**call-in** | **both**]	Required Call-in and call-out are allowed when the command is executed without any keyword.
Set the answer mode to auto answer.	**modem auto-answer**	Optional By default, manual answer mode is adopted.
Configure the carrier detection timeout time after off-hook during call-in connection setup	**modem timer answer** *seconds*	Optional 30 seconds by default.

Configuration Example

Enable Modem call-in and call-out, set the answer mode to auto answer, and set the timeout time to 45 seconds.

```
<SW7750> system-view
[SW7750] user-interface aux 0
[SW7750-ui-aux0] modem both
[SW7750-ui-aux0] modem auto-answer
[SW7750-ui-aux0] modem timer answer 45
```

6 LOGGING IN THROUGH THE WEB-BASED NETWORK MANAGEMENT SYSTEM

Introduction

A Switch 7750 has a Web server built in. It enables you to log into a Switch 7750 through a Web browser and then manage and maintain the switch intuitively by interacting with the built-in Web server.

To log into a Switch 7750 through the built-in Web-based network management system, you need to perform the related configuration on both the switch and the PC operating as the network management terminal.

Table 31 Requirements for logging into a switch through the Web-based network management system

Item	Requirement
Switch	The VLAN interface of the switch is assigned an IP address, and the route between the switch and the Web network management terminal is reachable. (Refer to "Configuring an IP Address for a VLAN Interface" on page 129 and "IP Routing Policy Configuration" on page 377 for related information.)
	The user name and password for logging into the Web-based network management system are configured.
PC operating as the network management terminal	IE is available.
	The IP address of the VLAN interface of the switch, the user name, and the password are available.

Establishing an HTTP Connection

1 Assign an IP address to VLAN-interface 1 of the switch (VLAN 1 is the default VLAN of the switch). See "Telneting to a Switch from a Terminal" on page 62 for related information.

2 Configure the user name and the password on the switch for the Web network management user to log in.

Create a Web user account, setting both the user name and the password to "admin" and the user level to 3.

```
<SW7750> system-view
[SW7750] local-user admin
[SW7750-luser-admin] service-type telnet level 3
[SW7750-luser-admin] password simple admin
```

3 Establish an HTTP connection between your PC and the switch, as shown in Figure 18.

Figure 18 Establish an HTTP connection between your PC and the switch



4 Log into the switch through IE. Launch IE on the Web-based network management terminal (your PC) and enter the IP address of the management VLAN interface of the switch in the address bar. (Make sure the route between the Web-based network management terminal and the switch is available.)

5 When the login authentication interface (as shown in Figure 19) appears, enter the user name and the password configured in step 2 and click <Login> to bring up the main page of the Web-based network management system.

Figure 19 The login page of the Web-based network management system



Configuring the Login Banner

Configuration Procedure

If a login banner is configured with the **header** command, when a user logs in through Web, the banner page is displayed before the user login authentication page. The contents of the banner page are the login banner information configured with the **header** command. Then, by clicking <Continue> on the banner page, the user can enter the user login authentication page, and enter the main page of the Web-based network management system after passing the authentication. If no login banner is configured by the **header** command, a user logging in through Web directly enters the user login authentication page.

Table 32 Configure the login banner

Operation	Command	Description
Enter system view	**system-view**	-
Configure the banner to be displayed when a user logs in through Web	**header login** *text*	Required By default, no login banner is configured.

Configuration Example

Network requirements

- A user logs in to the switch through Web.
- The banner page is desired when a user logs into the switch.

Network diagram

Figure 20 Network diagram for login banner configuration



Configuration Procedure

Enter system view.

```
<SW7750> system-view
```

Configure the banner "Welcome" to be displayed when a user logs into the switch through Web.

```
[SW7750] header login %Welcome%
```

Assume that a route is available between the user terminal (the PC) and the switch. After the above-mentioned configuration, if you enter the IP address of the switch in the address bar of the browser running on the user terminal and press <Enter>, the browser will display the banner page, as shown in Figure 21.

Figure 21 Banner page displayed when a user logs in to the switch through Web



Click <Continue> to enter user login authentication page. You will enter the main page of the Web-based network management system if the authentication succeeds.

Enabling/Disabling the WEB Server

Table 33 Enable/Disable the WEB Server

Operation	Command	Description
Enter system view	**system-view**	-
Enable the Web server	**ip http shutdown**	Required By default, the Web server is enabled.

Table 33 Enable/Disable the WEB Server

Operation	Command	Description
Disable the Web server	**undo ip http shutdown**	Required



To improve security and prevent attack to the unused Sockets, TCP 80 port (which is for HTTP service) is enabled/disabled after the corresponding configuration.

- *Enabling the Web server (by using the **undo ip http shutdown** command) opens TCP 80 port.*
- *Disabling the Web server (by using the **ip http shutdown** command) closes TCP 80 port.*

7 LOGGING IN THROUGH NMS

Introduction

You can also log into a switch through an NMS (network management station), and then configure and manage the switch through the agent module on the switch.

- The agent here refers to the software running on network devices (switches) and as the server.
- SNMP (simple network management protocol) is applied between the NMS and the agent.

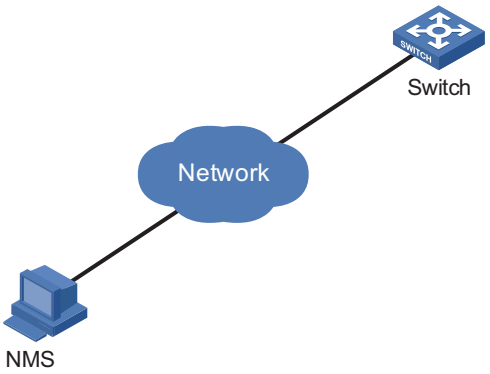
To log into a switch through an NMS, you need to perform related configuration on both the NMS and the switch.

Table 34 Requirements for logging into a switch through an NMS

Item	Requirement
Switch	The IP address of the VLAN interface of the switch is configured. The route between the NMS and the VLAN interface IP address is available. (Refer to "Configuring an IP Address for a VLAN Interface" on page 129 for more.)
	The basic SNMP functions are configured. (Refer to "Configuring SNMP Basic Functions" on page 741 for more.)
NMS	The NMS is properly configured. (Refer to the user manual of your NMS for more.)

Connection Establishment Using NMS

Figure 22 Network diagram for logging in through an NMS



8 USER CONTROL

Introduction

A switch provides ways to control different types of login users, as listed in Table 35.

Table 35 Ways to control different types of login users

Login mode	Control method	Implementation	Related section
Telnet	By source IP address	Through basic ACL	"Controlling Telnet Users by Source IP Addresses" on page 77
	By source and destination IP address	Through advanced ACL	"Controlling Telnet Users by Source and Destination IP Addresses" on page 78
SNMP	By source IP addresses	Through basic ACL	"Controlling Network Management Users by Source IP Addresses" on page 79
WEB	By source IP addresses	Through basic ACL	"Controlling Web Users by Source IP Address" on page 80
	Disconnect Web users by force	By executing commands in CLI	"Disconnecting a Web User by Force" on page 81

Controlling Telnet Users

Prerequisites: The controlling policy against Telnet users is determined, including the source and destination IP addresses to be controlled and the controlling actions (permitting or denying).

Controlling Telnet Users by Source IP Addresses

Controlling Telnet users by source IP addresses is achieved by applying basic ACLs, which are numbered from 2000 to 2999. For defining an ACL, refer to "Defining Basic ACLs" on page 641.

Table 36 Control Telnet users by source IP addresses

Operation	Command	Description
Enter system view	**system-view**	-
Create a basic ACL or enter basic ACL view	**acl** { **number** *acl-number* | **name** *acl-name* **basic** } [**match-order** { **config** | **auto** }]	As for the **acl number** command, the **config** keyword is specified by default.
Define rules for the ACL	**rule** [*rule-id*] { **permit** | **deny** } [**source** { *source-addr wildcard* | **any** | **fragment** | [**time-range** *time-name*]*	Required

Table 36 Control Telnet users by source IP addresses

Operation	Command	Description
Quit to system view	**quit**	-
Enter user interface view	**user-interface** [*type*] *first-number* [*last-number*]	-
Apply the ACL to control Telnet users by source IP addresses	**acl** *acl-number* { **inbound** | **outbound** }	Required The **inbound** keyword specifies to filter the users trying to Telnet to the current switch. The **outbound** keyword specifies to filter users trying to Telnet to other switches from the current switch.

Controlling Telnet Users by Source and Destination IP Addresses

Controlling Telnet users by source and destination IP addresses is achieved by applying advanced ACLs, which are numbered from 3000 to 3999. Refer to "Defining Advanced ACLs" on page 642.

Table 37 Control Telnet users by source and destination IP addresses

Operation	Command	Description
Enter system view	**system-view**	-
Create an advanced ACL or enter advanced ACL view	**acl** { **number** *acl-number* | **name** *acl-name* **advanced** } [**match-order** { **config** | **auto** }]	As for the **acl number** command, the **config** keyword is specified by default.
Define rules for the ACL	**rule** [*rule-id*] { **permit** | **deny** } *protocol* [**source** { *source-addr wildcard* | **any** }] [**destination** { *dest-addr dest-mask* | **any** }] [**source-port** *operator port1* [*port2*]] [**destination-port** *operator port1* [*port2*]] [**icmp-type** *type code*] [**established**] [[**precedence** *precedence* | **tos** *tos*]* | **dscp** *dscp*] [**fragment**] [**time-range** *time-name*]	Required You can define rules as needed to filter by specific source and destination IP addresses.
Quit to system view	**quit**	-
Enter user interface view	**user-interface** [*type*] *first-number* [*last-number*]	-
Apply the ACL to control Telnet users by specified source and destination IP addresses	**acl** *acl-number* { **inbound** | **outbound** }	Required The **inbound** keyword specifies to filter the users trying to Telnet to the current switch. The **outbound** keyword specifies to filter users trying to Telnet to other switches from the current switch.

Controlling Network Management Users by Source IP Addresses

You can manage a 3Com series Ethernet switch through network management software. Network management users can access switches through SNMP.

You need to perform the following two operations to control network management users by source IP addresses.

- Defining an ACL
- Applying the ACL to control users accessing the switch through SNMP

Prerequisites

The controlling policy against network management users is determined, including the source IP addresses to be controlled and the controlling actions (permitting or denying).

Controlling Network Management Users by Source IP Addresses

Controlling network management users by source IP addresses is achieved by applying basic ACLs, which are numbered from 2000 to 2999. For defining an ACL, refer to "Defining Basic ACLs" on page 641.

Table 38 Control network management users by source IP addresses

Operation	Command	Description
Enter system view	**system-view**	-
Create a basic ACL or enter basic ACL view	**acl** { **number** *acl-number* | **name** *acl-name* **basic** } [**match-order** { **config** | **auto** }]	As for the **acl number** command, the **config** keyword is specified by default.
Define rules for the ACL	**rule** [*rule-id*] { **permit** | **deny** } [**source** { *source-addr wildcard* | **any** } | **fragment** | **time-range** *time-name*]*	Required
Quit to system view	**quit**	-
Apply the ACL while configuring the SNMP community name	**snmp-agent community** { **read** | **write** } *community-name* [[**mib-view** *view-name*] | [**acl** *acl-number*]]*	Optional By default, SNMPv1 and SNMPv2c use community name to access.
Apply the ACL while configuring the SNMP group name	**snmp-agent group** { **v1** | **v2c** } *group-name* [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number*] **snmp-agent group v3** *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number*]	Optional By default, the authentication mode and the encryption mode are configured as none for the group.
Apply the ACL while configuring the SNMP user name	**snmp-agent usm-user** { **v1** | **v2c** } *user-name group-name* [**acl** *acl-number*] **snmp-agent usm-user v3** *user-name group-name* [**authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode des56** *priv-password*] [**acl** *acl-number*]	Optional

You can specify different ACLs while configuring the SNMP community name, the SNMP group name, and the SNMP user name.

As SNMP community name is a feature of SNMPv1 and SNMPv2c, the specified ACLs in the command that configures SNMP community names (the **snmp-agent community** command) take effect in the network management systems that adopt SNMPv1 or SNMPv2c.

Similarly, as SNMP group name and SNMP user are features of SNMPv2c and the higher SNMP versions, the specified ACLs in the commands that configure SNMP group names and SNMP user names take effect in the network management systems that adopt SNMPv2c or higher SNMP versions. If you specify ACLs in the two commands, the network management users are filtered by both SNMP group name and SNMP user name.

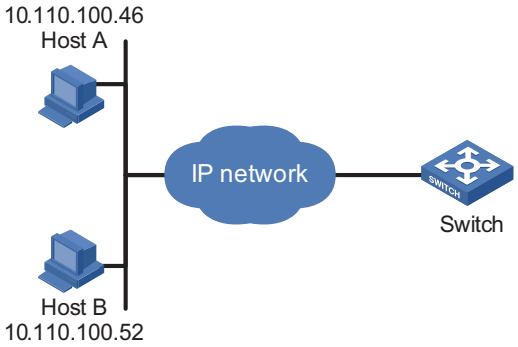
Configuration Example

Network requirements

Only SNMP users sourced from the IP addresses of 10.110.100.52 and 10.110.100.46 are permitted to access the switch.

Network diagram

Figure 23 Network diagram for controlling SNMP users using ACLs



Configuration procedure

Define a basic ACL.

```
<SW7750> system-view
[SW7750] acl number 2000 match-order config
[SW7750-acl-basic-2000] rule 1 permit source 10.110.100.52 0
[SW7750-acl-basic-2000] rule 2 permit source 10.110.100.46 0
[SW7750-acl-basic-2000] rule 3 deny source any
[SW7750-acl-basic-2000] quit
```

Apply the ACL to only permit SNMP users sourced from the IP addresses of 10.110.100.52 and 10.110.100.46 to access the switch.

```
[SW7750] snmp-agent community read aaa acl 2000
[SW7750] snmp-agent group v2c groupa acl 2000
[SW7750] snmp-agent usm-user v2c usera groupa acl 2000
```

Controlling Web Users by Source IP Address

You can manage a Switch 7750 remotely through Web. Web users can access a switch through HTTP connections.

You need to perform the following two operations to control Web users by source IP addresses.

- Defining an ACL
- Applying the ACL to control Web users

Prerequisites

The controlling policy against Web users is determined, including the source IP addresses to be controlled and the controlling actions (permitting or denying).

Controlling Web Users by Source IP Addresses

Controlling Web users by source IP addresses is achieved by applying basic ACLs, which are numbered from 2000 to 2999.

Table 39 Control Web users by source IP addresses

Operation	Command	Description
Enter system view	**system-view**	-
Create a basic ACL or enter basic ACL view	**acl number** *acl-number* [**match-order** { **config** | **auto** }]	As for the **acl number** command, the **config** keyword is specified by default.
Define rules for the ACL	**rule** [*rule-id*] { **deny | permit** } [*rule-string*]	Required
Quit to system view	**quit**	-
Apply the ACL to control Web users	**ip http acl** *acl-number*	Optional By default, no ACL is applied for Web users.

Disconnecting a Web User by Force

The administrator can disconnect a Web user by force using the related commands.

Table 40 Disconnect a Web user by force

Operation	Command	Description
Disconnect a Web user by force	**free web-users** { **all** | **user-id** *user-id* | **user-name** *user-name* }	Required Execute this command in user view.

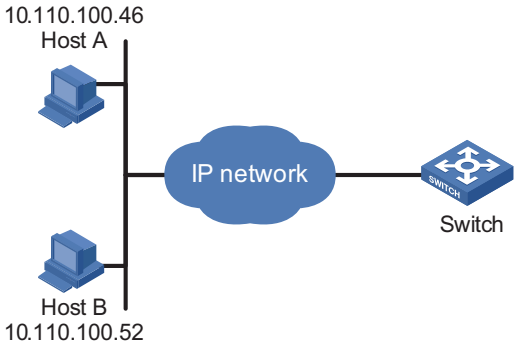
Configuration Example

Network requirements

Only the Web users sourced from the IP address of 10.110.100.52 are permitted to access the switch.

Network diagram

Figure 24 Network diagram for controlling Web users using ACLs



Configuration procedure

Define a basic ACL.

```
<SW7750> system-view
[SW7750] acl number 2030
[SW7750-acl-basic-2030] rule 1 permit source 10.110.100.52 0
[SW7750-acl-basic-2030] quit
```

Apply ACL 2030 to only permit the Web users sourced from the IP address of 10.110.100.52 to access the switch.

```
[SW7750] ip http acl 2030
```

9 CONFIGURATION FILE MANAGEMENT

Introduction to Configuration File

Configuration file records and stores user configurations performed to a switch. It also enables users to check switch configurations easily.

Upon powered on, a switch loads the configuration file known as saved-configuration file, which resides in the Flash, for initialization. If the Flash contains no configuration file, the system initializes using the default settings. Comparing to saved-configuration file, the configuration file which is currently adopted by a switch is known as the current-configuration.

A configuration file conforms to the following conventions:

- The content of a configuration files is a series of commands.
- Only the non-default configuration parameters are saved.
- The commands are grouped into sections by command view. The commands that are of the same command view are grouped into one section. Sections are separated by empty lines or comment lines. (A line is a comment line if it starts with the character "#".)
- The sections are listed in this order: system configuration section, logical interface configuration section, physical port configuration section, routing protocol configuration section, and so on.
- A configuration file ends with a "return".

Configuration File-Related Operations

You can perform the following operations on a Switch 7750:

- Saving the current configuration to a configuration file
- Removing a configuration file from the Flash
- Checking/Setting the configuration file to be used when the switch starts the next time

Perform the following configuration in user view.

Table 41 Configure a configuration file

Operation	Command	Description
Save the current configuration in Flash	**save** [*file-name* | **safely**]	Optional You can execute the **save** command in user view.

Table 41 Configure a configuration file

Operation	Command	Description
Remove a specific configuration file from the Flash	**reset saved-configuration**	Optional You can execute the **reset saved-configuration** command in user view.
Specify the configuration file to be used in the next startup	**startup saved-configuration** { *cfgfile* | *device-name* }	Optional You can execute the **start saved-configuration** command in user view.
Display the saved-configuration file	**display saved-configuration**	Optional You can execute the **display** command in any view.
Display the current configuration	**display current-configuration** [**interface** [*interface-type* [*interface-number*]] | **configuration** [*configuration*]] [**|** { **begin** | **exclude** | **include** } *text*]] | [**vlan** [*vlan-id*]]	
Display the configuration performed in the current view	**display this**	
Display the information about the configuration file to be used for startup.	**display startup**	

CAUTION: *Currently, the extension of a configuration file is cfg. Configuration files are saved in the root directory of the Flash.*

In the following conditions, it may be necessary for you to remove the configuration files from the Flash:

- The system software does not match the configuration file after the software of the Ethernet switch is updated.
- The configuration files in the Flash are damaged. The common reason is that wrong configuration files are loaded.

You can save the current configuration files in one of the following two ways:

- Fast saving mode: if the **safely** keyword is not provided, the system saves the configuration files in the fast saving mode. In this mode, the configuration files are saved fast. However, the original configuration files will be lost if the device is restarted or the power is off when the configuration files are being saved.
- Safely saving mode: if the **safely** keyword is provided, the system saves the configuration files in the safely saving mode. In this mode, the configuration files are saved slowly. However, the original configuration files will be saved in the Flash if the device is restarted or the power is off when the configuration files are being saved.

You are recommended to adopt the fast saving mode in the conditions of stable power and adopt the safe mode in the conditions of unstable power or remote maintenance.



- *You are recommended to use the **save** command to save the configuration before restarting a device, so that the current configuration remains after the device is restarted.*
- *If you use the **save** command to save the current configuration file without specifying any option, the configuration file is saved as the name of the configuration file used in this start. If the device is started using the default configuration file this time, the current configuration file is saved as the name of the default configuration file.*

10 VLAN OVERVIEW

VLAN Overview

Introduction to VLAN

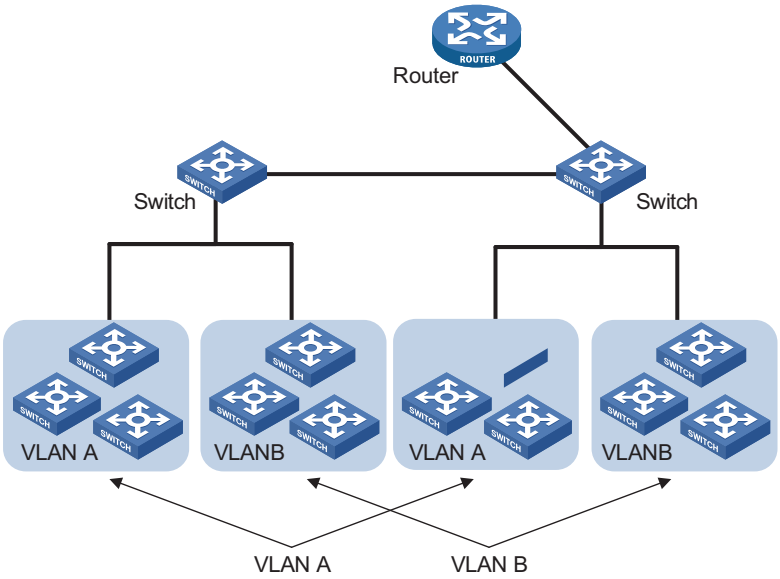
The traditional Ethernet is a flat network, where all hosts are in the same broadcast domain and connected with each other through hubs or switches. The hub is a physical layer device without the switching function, so it forwards the received packet to all ports. The switch is a link layer device which can forward the packet according to the MAC address of the packet. However, when the switch receives a broadcast packet or an unknown unicast packet whose MAC address is not included in the MAC address table of the switch, it will forward the packet to all the ports except the inbound port of the packet. In this case, a host in the network receives a lot of packets whose destination is not the host itself. Thus, plenty of bandwidth resources are wasted, causing potential serious security problems.

The traditional way to isolate broadcast domains is to use routers. However, routers are expensive and provide few ports, so they cannot subnet the network particularly.

The virtual local area network (VLAN) technology is developed for switches to control broadcast in LANs.

By creating VLANs in a physical LAN, you can divide the LAN into multiple logical LANs, each of which has a broadcast domain of its own. Hosts in the same VLAN communicate with each other as if they are in a LAN. However, hosts in different VLANs cannot communicate with each other directly. Figure 25 illustrates a VLAN implementation.

Figure 25 A VLAN implementation



A VLAN can span across multiple switches, or even routers. This enables hosts in a VLAN to be dispersed in a looser way. That is, hosts in a VLAN can belong to different physical network segment.

Compared with the traditional Ethernet, VLAN enjoys the following advantages.

- Broadcasts are confined to VLANs. This decreases bandwidth utilization and improves network performance.
- Network security is improved. VLANs cannot communicate with each other directly. That is, a host in a VLAN cannot access resources in another VLAN directly, unless routers or Layer 3 switches are used.
- Network configuration workload for the host is reduced. VLAN can be used to group specific hosts. When the physical position of a host changes within the range of the VLAN, you need not change its network configuration.

VLAN Principles

VLAN tags in the packets are necessary for the switch to identify packets of different VLANs. The switch works at Layer 2 (Layer 3 switches are not discussed in this chapter) and it can identify the data link layer encapsulation of the packet only, so you can add the VLAN tag field into only the data link layer encapsulation if necessary.

In 1999, IEEE issues the IEEE 802.1Q protocol to standardize VLAN implementation, defining the structure of VLAN-tagged packets.

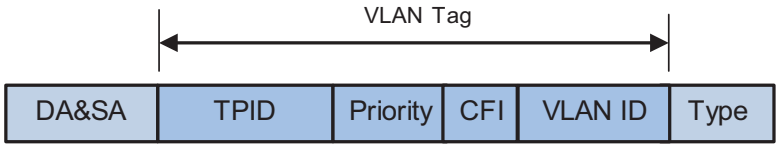
In traditional Ethernet data frames, the type field of the upper layer protocol is encapsulated after the destination MAC address and source MAC address, as shown in Figure 26

Figure 26 Encapsulation format of traditional Ethernet frames



In Figure 26 DA refers to the destination MAC address, SA refers to the source MAC address, and Type refers to the protocol type of the packet. IEEE 802.1Q protocol defines that a 4-byte VLAN tag is encapsulated after the destination MAC address and source MAC address to show the information about VLAN.

Figure 27 Format of VLAN tag



As shown in Figure 27, a VLAN tag contains four fields, including TPID, priority, CFI, and VLAN ID.

- TPID is a 16-bit field, indicating that this data frame is VLAN-tagged. By default, it is 0x8100 in 3Com series Ethernet switches.
- Priority is a 3-bit field, referring to 802.1p priority. Refer to "QoS Configuration" on page 657 for details.
- CFI is a 1-bit field, indicating whether the MAC address is encapsulated in the standard format in different transmission media. This field is not described in detail in this chapter.
- VLAN ID is a 12-bit field, indicating the ID of the VLAN to which this packet belongs. It is in the range of 0 to 4,095. Generally, 0 and 4,095 is not used, so the field is in the range of 1 to 4,094.

VLAN ID identifies the VLAN to which a packet belongs. When the switch receives an un-VLAN-tagged packet, it will encapsulate a VLAN tag with the default VLAN ID of the inbound port for the packet, and the packet will be assigned to the default VLAN of the inbound port for transmission.

Port-Based VLAN

Port-based VLAN technology introduces the simplest way to classify VLANs. You can isolate the hosts and divide them into different virtual workgroups through assigning the ports on the device connecting to hosts to different VLANs.

This way is easy to implement and manage and it is applicable to hosts with relatively fixed positions.

Link Types of Ethernet Ports

An Ethernet port on a Switch 7750 can be of the following three link types.

- Access. An access port can belong to only one VLAN. It is used to provide network access for terminal users.
- Trunk: A trunk port can belong to more than one VLAN. It can receive/send packets from/to multiple VLANs, and is generally used to connect another switch.
- Hybrid: A hybrid port can belong to more than one VLAN. It can receive/send packets from/to multiple VLANs, and can be used to connect either a switch or a user PC.

A hybrid port allows the packets of multiple VLANs to be sent without tags, but a trunk port only allows the packets of the default VLAN to be sent without tags.

You can configure all the three types of ports on the same device. However, note that you cannot directly switch a port between trunk and hybrid and you must set the port as access before the switching. For example, to change a trunk port to hybrid, you must first set it as access and then hybrid.

Adding an Ethernet Port to Specified VLANs

You can add the specified Ethernet port to a specified VLAN. After that, the Ethernet port can forward the packets of the specified VLAN, so that the VLAN on this switch can intercommunicate with the same VLAN on the peer switch.

An access port can only be added to one VLAN, while hybrid and trunk ports can be added to multiple VLANs.



The access ports or hybrid ports must be added to an existing VLAN.

Configuring the Default VLAN ID for an Ethernet Port

An Access port can belong to only one VLAN. Therefore, the VLAN an Access port belongs to is also the default VLAN of the Access port. A Hybrid/Trunk port can belong to several VLANs, and so a default VLAN ID for the port is required.

After a port is added to a VLAN and configured with a default VLAN, the port receives and sends packets in a way related to its link type. For detailed description, refer to Table 42, Table 43, and Table 44:

Table 42 Packet processing of an Access port

Processing of an incoming packet		
If the packet does not carry a VLAN tag	**If the packet carries a VLAN tag**	**Processing of an outgoing packet**
Receive the packet and add the default VLAN tag to the packet.	If the VLAN ID is just the default VLAN ID, receive the packet. If the VLAN ID is not the default VLAN ID, discard the packet.	Deprive the tag from the packet and send the packet.

Table 43 Packet processing of a Trunk port

Processing of an incoming packet		
If the packet does not carry a VLAN tag	**If the packet carries a VLAN tag**	**Processing of an outgoing packet**
If the port is already added to its default VLAN, add the default VLAN tag to the packet and then forward the packet. If the port is not added to its default VLAN, discard the packet.	If the VLAN ID is one of the VLAN IDs allowed to pass through the port, receive the packet. If the VLAN ID is not one of the VLAN IDs allowed to pass through the port, discard the packet.	If the VLAN ID is just the default VLAN ID, deprive the tag and send the packet. If the VLAN ID is not the default VLAN ID, keep the original tag unchanged and send the packet.

Table 44 Packet processing of a Hybrid port

Processing of an incoming packet		
If the packet does not carry a VLAN tag	**If the packet carries a VLAN tag**	**Processing of an outgoing packet**
If the port is already added to its default VLAN, add the default VLAN tag to the packet and then forward the packet. If the port is not added to its default VLAN, discard the packet.	If the VLAN ID is one of the VLAN IDs allowed to pass through the port, receive the packet. If the VLAN ID is not one of the VLAN IDs allowed to pass through the port, discard the packet.	Send the packet if the VLAN ID is allowed to pass through the port. Use the **port hybrid vlan** command to configure whether the port keeps or strips the tags when sending packets of a VLAN (including the default VLAN).

CAUTION: *You are recommended to set the default VLAN ID of the local Hybrid or Trunk ports to the same value as that of the Hybrid or Trunk ports on the peer switch. Otherwise, packet forwarding may fail on the ports.*

Protocol-Based VLAN

Introduction to Protocol-Based VLAN

Protocol-based VLAN is also known as protocol VLAN, which is another way to classify VLANs besides port-based VLAN. Through the protocol-based VLANs, the switch can analyze the received un-VLAN-tagged packets on the port and match the packets with the user-defined protocol template automatically according to different encapsulation formats and the values of the special fields. If a packet is matched, the switch will add a corresponding VLAN tag to it automatically. Thus, the data of the specific protocol is assigned automatically to the corresponding VLAN for transmission.

This feature is used for binding the ToS provided in the network to VLAN to facilitate management and maintenance.

Encapsulation Format of Ethernet Data

This section introduces the common encapsulation formats of Ethernet data for you to understand well the procedure for the switch to identify the packet protocols.

Ethernet II and 802.2/802.3 encapsulation

In the link layer, there are two main packet encapsulation types: Ethernet II and 802.2/802.3, whose encapsulation formats are described in the following figures.

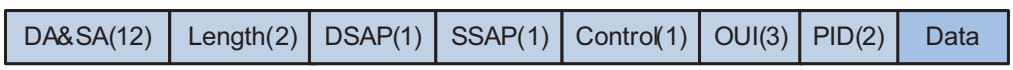
Ethernet II packet:

Figure 28 Ethernet II encapsulation format



802.2/802.3 standard packet:

Figure 29 802.2/802.3 standard encapsulation format



In the two figures, DA and SA refer to the destination MAC address and source MAC address of the packet respectively. The number in the bracket indicates the field length in bits.

The maximum length of an Ethernet packet is 1500 bytes, that is, 5DC in hexadecimal, so the length field in 802.2/802.3 encapsulation is in the range of 0x0000 to 0x05DC.

Whereas, the type field in Ethernet II encapsulation is in the range of 0x0600 to 0xFFFF.

The switch identifies whether a packet is an Ethernet II packet or an 802.2/802.3 packet according to the ranges of the two fields.

Encapsulation formats of 802.2/802.3 packets

802.2/802.3 packets are encapsulated in the following three formats:

- 802.3 raw encapsulation: only the length field is encapsulated after the source and destination address field, followed by the upper layer data. The type field is not included.

Figure 30 802.3 raw encapsulation format



Only the IPX protocol supports 802.3 raw encapsulation format currently. This format is identified by the two bytes whose value is 0xFFFF after the length field.

- 802.2 logical link control (LLC) encapsulation: the length field, the destination service access point (DSAP) field, the source service access point (SSAP) field and the control field are encapsulated after the source and destination address field.

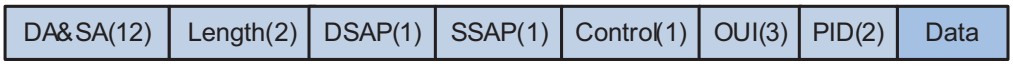
Figure 31 802.2 LLC encapsulation format



The DSAP field and the SSAP field in the LLC part are used to identify the upper layer protocol. For example, the two fields are both 0xE0, meaning that the upper layer protocol is IPX protocol.

- 802.2 sub-network access protocol (SNAP) encapsulation: the length field, the DSAP filed, the SSAP field, the control field, the OUI field and the PID field are encapsulated according to 802.2/802.3 standard packets.

Figure 32 802.2 SNAP encapsulation format



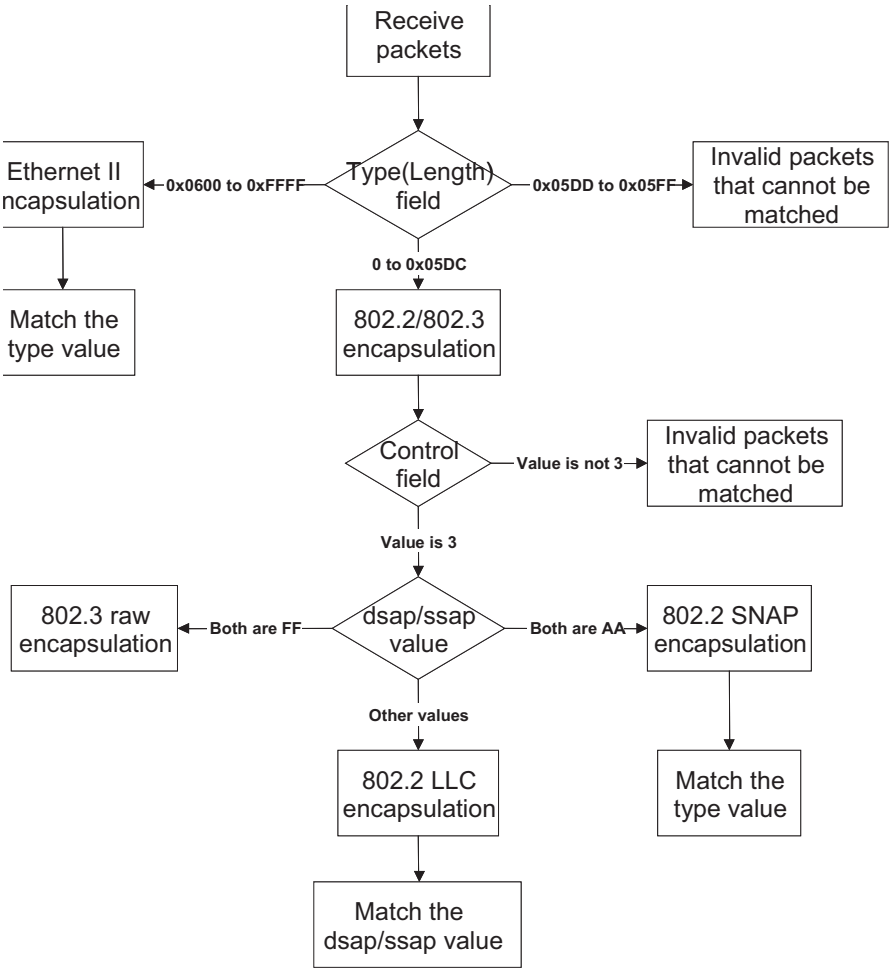
In 802.2 SNAP encapsulation format, the values of the DSAP field and the SSAP field are always AA, and the value of the control field is always 3.

The switch differentiates between 802.2 LLC encapsulation and 802.3 SNAP encapsulation according to the values of the DSAP field and the SSAP field.

When the OUI is 00-00-00 in 802.2 SNAP encapsulation, the PID field has the same meaning as the type field in Ethernet II encapsulation, which both refer to globally unique protocol number. Such encapsulation is also known as SNAP RFC1042 encapsulation, which is standard SNAP encapsulation. The SNAP encapsulation mentioned in this chapter refers to SNAP RFC 1042 encapsulation.

Procedure for the Switch to Judge Packet Protocol

Figure 33 Procedure for the switch to judge packet protocol



Encapsulation Formats

Table 45 Encapsulation formats

Encap	Protocol	Ethernet II	802.3 raw	802.2 LLC	802.2 SNAP	Type value
IP	Supported	Not supported	Not supported	Supported	0x0800	
IPX	Supported	Supported	Supported	Supported	0x8137	
AppleTalk	Supported	Not supported	Not supported	Supported	0x809B	

Implementation of Protocol-Based VLAN

Switch 7750 Ethernet switches assign the packet to the specific VLAN by matching the packet with the protocol template.

The protocol template is the standard to determine the protocol to which a packet belongs. Protocol templates include standard templates and user-defined templates:

- The standard template adopts the RFC- or IEEE-defined packet encapsulation formats and values of some specific fields as the matching criteria.
- The user-defined template adopts the user-defined encapsulation formats and values of some specific fields as the matching criteria.

After configuring the protocol template, you must add a port to the protocol-based VLAN and associate this port with the protocol template. This port will add VLAN tags to the packets based on protocol types. The port in the protocol-based VLAN must be connected to a client. However, a common client cannot process VLAN-tagged packets. In order that the client can process the packets out of this port, you must configure the port in the protocol-based VLAN as a hybrid port and configure the port to remove VLAN tags when forwarding packets of all VLANs.

11 VLAN CONFIGURATION

VLAN Configuration

Basic VLAN Configuration

Table 46 Basic VLAN configuration

Operation	Command	Description
Enter system view	**system-view**	-
Create a VLAN and enter VLAN view	**vlan** *vlan-id*	Required The *vlan-id* argument ranges from 1 to 4,094.
Assign a name for the current VLAN	**name** *string*	Optional By default, the name of a VLAN is its VLAN ID.
Specify the description string of the current VLAN	**description** *string*	Optional By default, the description string of a VLAN is its VLAN ID.

Create a Range of VLANs

You can use the following command to create a range of VLANs, reducing your workload of creating VLANs.

Table 47 Create a range of VLANs

Operation	Command	Remarks
Enter system view	**system-view**	-
Create a ranges of VLANs	**vlan** *vlan-id1* **to** *vlan-id2*	Required
Create all VLANs	**vlan all**	Optional



CAUTION: *As the default VLAN, VLAN 1 needs not to be created and cannot be removed.*

Configuring VLAN Broadcast Storm Suppression

You can use the following command to set the maximum volume of allowed broadcast traffic through a VLAN. When the actual broadcast traffic exceeds the specified value, the system will discard the extra packets so that the bandwidth occupied by broadcast traffic can be kept within a specific ratio. In this way, the system can suppress broadcast storm, avoid network congestion and ensure normal network operation.

Table 48 Configure VLAN broadcast storm suppression

Operation	Command	Description
Enter system view	**system-view**	-

Table 48 Configure VLAN broadcast storm suppression

Operation	Command	Description
Enter VLAN view	**vlan** *vlan-id*	-
Set VLAN broadcast storm suppression	**broadcast-suppression** { *ratio* | **pps** *pps* }	Required

A VLAN only supports one broadcast storm suppression mode at one time. If you configure broadcast storm suppression modes multiple times for a VLAN, the latest configuration will overwrite the previous configuration.

Different modules of Switch 7750s support different broadcast storm suppression modes, as listed in Table 49.

Table 49 Broadcast storm suppression modes and module types

VLAN broadcast storm suppression mode	Type A cards	Other cards
VLAN pps suppression	Supported	Not supported
VLAN bandwidth ratio suppression	Supported	Not supported

Type A modules include 3C16860, 3C16861, LS81FS24A, 3C16858, 3C16859, and 32Gbps and 64Gbps Switch Fabrics.

Basic VLAN Interface Configuration

Configuration prerequisites

Create a VLAN before configuring a VLAN interface.

Configuration procedure

Table 50 Basic VLAN interface configuration

Operation	Command	Description
Enter system view	**system-view**	-
Create a VLAN interface and enter VLAN interface view	**interface Vlan-interface** *vlan-id*	Required The *vlan-id* argument ranges from 1 to 4,094.
Specify the description string for the current VLAN interface	**description** *text*	Optional By default, the description string of a VLAN interface is the name of this VLAN interface
Disable the VLAN interface	**shutdown**	Optional
Enable the VLAN Interface	**undo shutdown**	By default, a VLAN interface is enabled.

Note that the operation of enabling/disabling a VLAN interface does not influence the enabling/disabling states of the Ethernet ports belonging to this VLAN.

By default, a VLAN interface is enabled. In this scenario, the VLAN interface's status is determined by the status of its ports, that is, if all the ports of the VLAN interface are down, the VLAN interface is down (disabled); if one or more ports of the VLAN interface are up, the VLAN interface is up (enabled).

If a VLAN interface is disabled, its status is not determined by the status of its ports.

Displaying VLAN Configuration

After the configuration above, you can execute the **display** command in any view to display the running status after the configuration, so as to verify the configuration.

Table 51 Display VLAN configuration

Operation	Command	Description
Display the VLAN interface information	**display interface Vlan-interface** [*vlan-id*]	You can execute the **display** command in any view.
Display the VLAN information	**display vlan** [*vlan-id* [**to** *vlan-id*] | **all** | **static** | **dynamic**]	

Configuring a Port-Based VLAN

Configuring an Access-Port-Based VLAN

There are two ways to configure Access-port-based VLAN: one way is to configure in VLAN view, the other way is to configure in Ethernet port view.

Follow these steps to configure the Access-port-based VLAN in VLAN view:

To do...	Use the command...	Remarks
Enter system view	**system-view**	-
Enter VLAN view	**vlan** *vlan-id*	Required If the specified VLAN does not exist, this command be created first creates the VLAN before entering its view.
Add an Access port to the current VLAN	**port** *interface-list*	Required By default, system will add all ports to VLAN 1.

Follow these steps to configure the Access-port-based VLAN in Ethernet port view:

To do...	Use the command...	Remarks
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Configure the port link type as Access	**port link-type access**	Optional The link type of a port is Access by default.
Add the current Access port to a specified VLAN	**port access vlan** *vlan-id*	Optional By default, all Access ports belong to VLAN 1.



To add an Access port to a VLAN, make sure the VLAN already exists.

Configuring a Hybrid-Port-Based VLAN

A Hybrid port may belong to multiple VLANs, and this configuration can only be performed in Ethernet port view.

Follow these steps to configure the Hybrid-port-based VLAN:

To do...	Use the command...	Remarks
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Configure the port link type as Hybrid	**port link-type hybrid**	Required
Configure the default VLAN of the Hybrid port	**port hybrid pvid vlan** *vlan-id*	Optional VLAN 1 is the default by default
Allow the specified VLANs to pass through the current Hybrid port	**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	Required By default, all Hybrid ports only allow packets of VLAN 1 to pass.

- *To configure a Trunk port into a Hybrid port (or vice versa), you need to use the Access port as a medium. For example, the Trunk port has to be configured as an Access port first and then a Hybrid port.*
- *Ensure that the VLANs already exist before configuring them to pass through a Hybrid port.*
- *The default VLAN IDs of the Hybrid ports on the local and the peer devices must be the same. Otherwise, packets cannot be transmitted properly.*

Configuring a Trunk-Port-Based VLAN

A Trunk port may belong to multiple VLANs, and you can only perform this configuration in Ethernet port view.

Follow these steps to configure the Trunk-port-based VLAN:

To do...	Use the command...	Remarks
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Configure the port link type as Trunk	**port link-type trunk**	Required
Configure the default VLAN for the Trunk port	**port trunk pvid vlan** *vlan-id*	Optional VLAN 1 is the default by default.
Allow the specified VLANs to pass through the current Trunk port	**port trunk permit vlan** { *vlan-id-list* | **all** }	Required By default, all Trunk ports only allow packets of VLAN 1 to pass.

- *To convert a Trunk port into a Hybrid port (or vice versa), you need to use the Access port as a medium. For example, the Trunk port has to be configured as an Access port first and then a Hybrid port.*

- *The default VLAN IDs of the Trunk ports on the local and peer devices must be the same. Otherwise, packets cannot be transmitted properly.*

Displaying and Maintaining Port-Based VLAN

To do...	Use the command...	Remarks
Display the hybrid or trunk ports	**display port** { **hybrid** | **trunk** }	Available in any view.

Configuring a Port-Based VLAN

Configuration prerequisites

Create a VLAN before configuring a port-based VLAN.

Configuration procedure

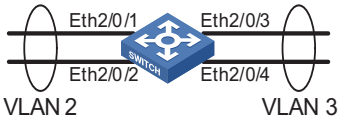
Port-based VLAN Configuration Example

Configuration requirements

- Create VLAN 2 and VLAN 3 and specify the description string of VLAN 2 as home;
- Add Ethernet2/0/1 and Ethernet2/0/2 to VLAN 2 and add Ethernet2/0/3 and Ethernet2/0/4 to VLAN 3.

Network diagram

Figure 34 Network diagram for VLAN configuration



Configuration procedure

Create VLAN 2 and enter its view.

```
<SW7750> system-view
[SW7750] vlan 2
```

Specify the description string of VLAN 2 as home.

```
[SW7750-vlan2] description home
```

Add Ethernet2/0/1 and Ethernet2/0/2 ports to VLAN 2.

```
[SW7750-vlan2] port Ethernet2/0/1 Ethernet2/0/2
```

Create VLAN 3 and enter its view.

```
[SW7750-vlan2] quit
[SW7750]vlan 3
```

Add Ethernet2/0/3 and Ethernet2/0/4 ports to VLAN 3.

```
[SW7750-vlan3] port Ethernet2/0/3 Ethernet2/0/4
```

Configuring a Protocol-Based VLAN

Creating Protocol Template for Protocol-Based VLAN

Configuration prerequisites

Create a VLAN before configuring a protocol-based VLAN.

Configuration procedure

Table 52 Create protocol types of VLANs

Operation	Command	Description
Enter system view	**system-view**	-
Enter VLAN view	**vlan** *vlan-id*	Required
Create the protocol template for the VLAN	**protocol-vlan** [*protocol-index*] { **at** | **ip** [*ip-address* [*net-mask*]] | **ipx** { **ethernetii** | **llc** | **raw** | **snap** } | **mode** { **ethernetii** [**etype** *etype-id*] | **llc** { **dsap** *dsap-id* [**ssap** *ssap-id*] | **ssap** *ssap-id* } | **snap** [**etype** *etype-id*] }}	Required

When you are creating protocol templates for protocol-based VLANs, the **at**, **ip** and **ipx** keywords are used to create standard templates, and the **mode** keyword is used to create user-defined templates.



CAUTION: *In a VLAN, it is not allowed to configure two templates with the same protocol type and encapsulation format. If any parameter in a user-defined template has the same value as the corresponding parameter in the standard template, the user-defined template and the standard template cannot be configured in the same VLAN.*

Pay attention to the following notices about the template configuration

- *It is not allowed to configure both **ipx llc** standard template and LLC user-defined template whose dsap-id and ssap-id are both 0xe0 in the same VLAN.*
- *It is not allowed to configure both **ipx raw** standard template and LLC user-defined template whose **dsap** and **ssap** are both ff in the same VLAN.*
- *It is not allowed to configure both **ipx ethernetii** standard template and EthernetII user-defined template whose **etype** is 8137 in the same VLAN.*
- *It is not allowed to configure both **ipx snap** standard template and SNAP user-defined template whose **etype** is 8137 in the same VLAN.*
- *When the values of the dsap-id and ssap-id arguments are AA, the packet encapsulation type is not **llc** but **snap**. To avoid template conflict, the system disable the value AA for the dsap-id and ssap-id arguments when you configure LLC user-defined template.*

In addition, pay attention to the following notices about IP template

- *If a packet can match both Ipv4-based VLAN and the VLAN based on other protocol, Ipv4-based VLAN takes higher priority.*

- ***ip*** *[ip-address [net-mask]] defines IPv4-based VLAN. If you want to define the VLANs based on IP or other encapsulation formats, use* ***mode*** *{* ***ethernetii*** *[* ***etype*** *etype-id] } and* ***snap*** *[* ***etype*** *etype-id], in which, etype-id is 0x0800.*

Associating a Port with the Protocol-Based VLAN

Configuration prerequisites

- The protocol template for the protocol-based VLAN is created
- The port is configured as a hybrid port, and the port is configured to remove VLAN tags when it forwards the packets of the protocol-based VLANs.

Configuration procedure

Table 53 Associate a port with the protocol-based VLAN

Operation	Command	Description
Enter system view	**system-view**	-
Enter port view	**interface** *interface-type interface-number*	-
Associate a port with the protocol-based VLAN	**port hybrid protocol-vlan vlan** *vlan-id* { *protocol-index* [**to** *protocol-end*] | **all** }	Required

CAUTION:

- *For the same VLAN, it is not allowed to configure the same protocol type and encapsulation format. Between different VLANs, the same protocol type and encapsulation format can be configured, but cannot be distributed to the same port. Even the user-defined template and standard template with the same encapsulation format cannot be distributed to the same port.*
- *If a protocol template has been configured in a VLAN, the VLAN cannot be removed.*
- *If a protocol of a VLAN has been distributed to a port, the VLAN cannot be removed from the port.*
- *If a protocol of a VLAN has been distributed to a port, the protocol cannot be removed from the VLAN.*
- *For a given type of packets, if the protocol VLAN bound to a port is different from the protocol VLAN applied on the module that provides the port, the board-associated protocol VLAN configuration supersedes the port-associated protocol VLAN configuration.*

Associating a Module with the Protocol-Based VLAN

Table 54 Create/Remove protocol-based VLAN on specific card

Operation	Command	Description
Enter system view	**system-view**	-
Create protocol-based VLAN on specific card	**protocol-vlan vlan** *vlan-id* { *protocol-index* [**to** *protocol-end*] | **all** } { **slot** *slot-number* | **mainboard** }	Required

CAUTION:

- *It is necessary to add those ports that require protocol on the module to the protocol-based VLAN.*

- *Currently, only non-Type-A modules, including I/O Modules and Fabric, support this command.*
- *If a protocol-based VLAN has been associated with a module, the VLAN cannot be removed.*
- *If a protocol in a VLAN has been associated with a module, the protocol cannot be removed from the VLAN.*
- *For a given type of packets, if the protocol VLAN bound to a port is different from the protocol VLAN applied on the module that provides the port, the board-associated protocol VLAN configuration supersedes the port-associated protocol VLAN configuration.*

Table 55 shows the supported protocol-based VLAN creation on different I/O Modules.

Table 55 Protocol-based VLAN creation on different cards

Description	Type A card	Non-Type-A card
Create protocol-based VLAN on specific module in system view.	Not supported	Supported (only for all IP protocols and subnet IP protocols).
Create protocol-based VLAN on specific port in Ethernet port view.	Supported	Supported (exclude all IP protocols and subnet IP protocols, AppleTalk protocol, and the user-defined LLC template which defines only one of *dsap-id* and *ssap-id*).



Type A modules include 3C16860, 3C16861, LS81FS24A, 3C16858, 3C16859, and 32Gbps and 64Gbps Switch Fabrics.

Displaying Protocol-Based VLAN Configuration

After the configuration above, you can execute the **display** command in any view to display the running status, so as to verify the configuration.

Table 56 Display VLAN configuration

Operation	Command	Description
Display the information about the protocol-based VLAN	**display vlan** [*vlan-id* [**to** *vlan-id*] | **all** | **static** | **dynamic**]	You cam **execute** the display command in any view
Display the protocol information and protocol indexes configured on the specified VLAN	**display protocol-vlan vlan** { *vlan-id* [**to** *vlan-id*] | **all** }	
Display the protocol information and protocol indexes configured on the specified port	**display protocol-vlan interface** { *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	
Display protocol-based VLAN information on specific card	**display protocol-vlan slot** { *slot-number* [**to** *slot-number*] | **all** }	

Protocol-Based VLAN Configuration Example

Standard-template-protocol-based VLAN configuration example

1 Network requirements

- Create VLAN 5 and configure it to be a protocol-based VLAN, with the protocol-index being 1 and the protocol being IP.
- Associate Ethernet2/0/5 port with the protocol-based VLAN to enable IP packets received by this port to be tagged with the tag of VLAN 5 and be transmitted in VLAN 5.

2 Configuration procedure

Create VLAN 5 and enter its view.

```
<SW7750> system-view
[SW7750] vlan 5
[SW7750-vlan5]
```

Configure the protocol-index to be 1, and the associated protocol to be IP.

```
[SW7750-vlan5] protocol-vlan 1 ip
```

Enter Ethernet2/0/5 port view.

```
[SW7750-vlan5] interface Ethernet 2/0/5
```

Configure the port to be a hybrid port.

```
[SW7750-Ethernet2/0/5] port link-type hybrid
```

Add the port to VLAN 5 and add VLAN 5 to the untagged VLAN list of the port.

```
[SW7750-Ethernet2/0/5] port hybrid vlan 5 untagged
```

Associate the port with protocol-index 1.

```
[SW7750-Ethernet2/0/5] port hybrid protocol-vlan vlan 5 1
```

User-defined-template-based protocol VLAN configuration example

1 Network requirement

- Create VLAN 7 and configure it as a protocol-based VLAN.
- Create two indexes in VLAN 7. Index 1 is used to match the packets with DSAP and SSAP value being 01 and ac respectively in 802.2 LLC encapsulation; Index 2 is used to match the packets with the Type value being 0xabcd in 802.2 SNAP encapsulation.
- Associate Ethernet2/0/7 with the two indexes of the protocol-based VLAN 7. When packets matching one of the indexes are received by Ethernet2/0/7, the packets will be tagged with the tag of VLAN 7 automatically.

2 Configuration procedure

Create VLAN 7 and enter its view.

```
<SW7750> system-view
[SW7750] vlan 7
[SW7750-vlan7]
```

Configure index 1 of VLAN 7 according to the network requirement.

```
[SW7750-vlan7] protocol-vlan 1 mode llc dsap 01 ssap ac
```

Configure index 2 of VLAN 7 according to the network requirement.

```
[SW7750-vlan7] protocol-vlan 2 mode snap etype abcd
```

Enter port view of the Ethernet2/0/7.

```
[SW7750-vlan7] interface Ethernet 2/0/7
```

Configure Ethernet2/0/7 as a hybrid port.

```
[SW7750-Ethernet2/0/7] port link-type hybrid
```

Add the port to VLAN 7, and add VLAN 7 to the list of untagged VLANs permitted to pass through the port.

```
[SW7750-Ethernet2/0/7] port hybrid vlan 7 untagged
```

Associate the port with the two indexes of VLAN 7.

```
[SW7750-Ethernet2/0/7] port hybrid protocol-vlan vlan 7 1 to 2
```

12 VOICE VLAN CONFIGURATION

Voice VLAN Overview

Voice VLANs are VLANs configured specially for voice data stream. By adding the ports with voice devices attached to voice VLANs, you can perform QoS (quality of service)-related configuration for voice data, ensuring the transmission priority of voice data stream and voice quality.

Switch 7750 Ethernet switches determine whether a received packet is a voice packet by checking its source MAC address. If the source MAC addresses of packets comply with the organizationally unique identifier (OUI) addresses configured by the system, the packets are determined as voice packets and transmitted in voice VLAN.

You can configure an OUI address for voice packets or specify to use the default OUI address.



An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of a MAC address.

The following table shows the five default OUI addresses of a switch.

Table 57 Default OUI addresses preset by the switch

Number	OUI Address	Vendor
1	0003-6b00-0000	Cisco phone
2	000f-e200-0000	3Com Aolynk phone
3	00d0-1e00-0000	Pingtel phone
4	00e0-7500-0000	Polycom phone
5	00e0-bb00-0000	3com phone

You can create multiple voice VLANs and bind each voice VLAN to a port. In this way, the voice traffic received by a port can be transmitted in the voice VLAN bound to the port. This feature allows you to manage voice traffic flexibly.

A voice VLAN can operate in two modes: automatic mode and manual mode. You can configure the operation mode for a voice VLAN according to data stream passing through the ports of the voice VLAN.

- In automatic mode: Switch 7750s automatically add a port connecting a IP voice device to the voice VLAN through learning the source MAC address in the untagged packet sent by the IP voice device when it is powered on. When the aging time of a port expires, voice ports on which the OUI addresses are not updated (no voice stream passes) will be automatically removed from the voice

VLAN; voice ports cannot be added into or removed from the voice VLAN through manual configurations.

- In manual mode: you need to execute related configuration commands to add a voice port to the voice VLAN or remove a voice port from the voice VLAN.

Tagged packets from IP voice devices are forwarded based on their tagged VLAN IDs, whether the automatic or manual mode is used.

Voice VLAN packets can be forwarded by trunk ports and hybrid ports in voice VLAN. You can enable a trunk port or a hybrid port belonging to other VLANs to forward voice and service packets simultaneously by enabling the voice VLAN function for it.

As multiple types of IP voice devices exist, you need to match port mode with types of voice stream sent by IP voice devices, as listed in Table 58.

Table 58 Matching relationship between port modes and voice stream types

Port voice VLAN mode	Voice stream type	Port type	Supported or not
Automatic mode	Tagged voice stream	Access	Not supported
		Trunk	Supported Make sure the default VLAN of the port exists and is not a Voice VLAN. And the access port permits the packets of the default VLAN.
		Hybrid	Supported Make sure the default VLAN of the port exists and is in the list of the tagged VLANs whose packets are permitted by the access port.
	Untagged voice stream	Access	Not supported, because the default VLAN of the port must be a voice VLAN and the access port is in the voice VLAN. To do so, you can also add the port to the voice VLAN manually.
		Trunk	
		Hybrid	

Table 58 Matching relationship between port modes and voice stream types

Port voice VLAN mode	Voice stream type	Port type	Supported or not
Manual mode	Tagged voice stream	Access	Not supported
		Trunk	Supported Make sure the default VLAN of the port exists and is not a voice VLAN. And the access port permits the packets of the default VLAN.
		Hybrid	Supported Make sure the default VLAN of the port exists and is in the list of the tagged VLANs whose packets are permitted by the access port.
	Untagged voice stream	Access	Supported Make sure the default VLAN of the port is a voice VLAN.
		Trunk	Supported Make sure the default VLAN of the port is a voice VLAN and the port permits the packets of the VLAN.
		Hybrid	Supported Make sure the default VLAN of the port is a voice VLAN and is in the list of untagged VLANs whose packets are permitted by the port.



CAUTION: *If the voice stream transmitted by an IP voice device is with VLAN tag and the port which the IP voice device is attached to is enabled with 802.1x authentication and 802.1x guest VLAN, assign different VLAN IDs for the voice VLAN bound to the port, the default VLAN of the port, and the 802.1x guest VLAN to ensure the two functions to operate properly.*

Voice VLAN Configuration

Configuration Prerequisites

- Create the corresponding VLAN before configuring a voice VLAN.
- As the default VLAN, VLAN 1 cannot be bound to a port as a voice VLAN.

Configuring a Voice VLAN to Operate in Automatic Mode

Table 59 Configure a voice VLAN to operate in automatic mode

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	Required
Enable the voice VLAN function for the port	**voice vlan enable**	Required By default, the voice VLAN function is disabled.
Bind a VLAN to the port as a voice VLAN	**voice vlan** *vlan-id*	Required By default, no voice VLAN is bound to a port.
Enable the voice VLAN legacy function on the port	**voice vlan legacy**	Optional By default, voice VLAN legacy is disabled.
Set the voice VLAN operation mode to automatic mode	**voice vlan mode auto**	Optional The default voice VLAN operation mode is automatic mode.
Quit to system view	**quit**	-
Set an OUI address that can be identified by the voice VLAN	**voice vlan mac-address** *oui* **mask** *oui-mask* [**description** *text*]	Optional By default, the switch uses the default OUI address to determine the voice stream.
Enable the voice VLAN security mode	**voice vlan security enable**	Optional By default, the voice VLAN security mode is enabled.
Set the aging time for the voice VLAN	**voice vlan aging** *minutes*	Optional The default aging time is 1,440 minutes.

For a port operating in automatic mode, a default VLAN cannot be configured as a voice VLAN; otherwise the system prompts you for unsuccessful configuration.

Configuring a voice VLAN to operate in manual mode

Table 60 Configure a voice VLAN to operate in manual mode

Operation	Command	Description
Enter system view	**system-view**	-
Enter port view	**interface** *interface-type interface-number*	Required

Table 60 Configure a voice VLAN to operate in manual mode

Operation			Command	Description
Enable the voice VLAN function for the port			**voice vlan enable**	Required By default, the voice VLAN function is disabled on a port.
Bind a VLAN to the port as a voice VLAN			**voice vlan** *vlan-id*	Required By default, no voice VLAN is bound to a port.
Enable the voice VLAN legacy function on the port			**voice vlan legacy**	Optional By default, voice VLAN legacy is disabled.
Set voice VLAN operation mode to manual mode			**undo voice vlan mode auto**	Required The default voice VLAN operation mode is automatic mode.
Quit to system view			**quit**	-
Add a port in manual mode to the voice VLAN	Access port	Enter VLAN view	**vlan** *vlan-id*	Required
		Add the port to the VLAN	**port** *interface-list*	
	Trunk or Hybrid port	Enter port view	**interface** *interface-type interface-number*	
		Add the port to the voice VLAN	**port trunk permit vlan** *vlan-id* **port hybrid vlan** *vlan-id* { **tagged** | **untagged** }	
		Configure the voice VLAN to be the default VLAN of the port	**port trunk pvid vlan** *vlan-id* **port hybrid pvid vlan** *vlan-id*	Optional Refer to Table 58 to determine whether or not this operation is needed.
Quit to system view			**quit**	-
Set an OUI address to be one that can be identified by the voice VLAN			**voice vlan mac-address** *oui* **mask** *oui-mask* [**description** *text*]	Optional If you do not set the address, the default OUI address is used.
Enable the voice VLAN security mode			**voice vlan security enable**	Optional By default, the voice VLAN security mode is enabled.
Set aging time for the voice VLAN			**voice vlan aging** *minutes*	Optional The default aging time is 1,440 minutes.

CAUTION:

- *If the Link Aggregation Control Protocol (LACP) is enabled for a port, the voice VLAN feature can not be enabled for it.*

- *Voice VLAN function can be effective only for the static VLAN. Once a dynamic VLAN is enabled with voice VLAN function, it automatically changes to static VLAN.*
- *When a voice VLAN operates in the security mode, the devices in it only permit packets whose source addresses are the voice OUI addresses that can be identified. Packets whose source addresses cannot be identified, including certain authentication packets (such as 802.1x authentication packets), will be dropped. So, do not transmit both voice data and service data in a voice VLAN. If you have to do so, make sure the voice VLAN do not operate in the security mode.*
- *After the voice VLAN function is enabled on a port, you cannot enable the QinQ feature on the port, and vice versa, that is, after the QinQ feature is enabled on a port, you cannot enable the voice VLAN function on the port.*
- *A voice VLAN-enabled port will automatically learn OUI addresses, without being limited by the function of prohibiting MAC address learning and the specified maximum number of MAC addresses to be learnt.*
- *The voice VLAN legacy feature realizes the communication between 3Com's devices and other vendor's voice devices by automatically adding the voice VLAN tag to the voice data coming from other vendors' voice devices. The **voice vlan legacy** command can be executed before voice VLAN is enabled globally and on a port, but it takes effect only after voice VLAN is enabled globally and on the port.*

Displaying and Maintaining Voice VLAN Configuration

After the above configurations, you can execute the **display** command in any view to view the running status and verify the configuration effect.

Table 61 Display configurations of a Voice VLAN

Operation	Command	Description
Display the voice VLAN configuration status	**display voice vlan status**	You can execute the **display** command in any view.
Display the currently valid OUI addresses	**display voice vlan oui**	
Display the ports operating in the current voice VLAN	**display vlan** *vlan-id*	

Voice VLAN Configuration Example

Voice VLAN Configuration Example (Automatic Mode)

Network requirements

- Configure Ethernet2/0/1 port as a Trunk port, with VLAN 6 as the default port. Bind VLAN 2 to Ethernet 2/0/1 as a voice VLAN.
- Ethernet2/0/1 port can be added to/removed from the voice VLAN automatically according to the type of the data stream that reaches the port.

Configuration procedure

Create VLAN 2.

```
<SW7750> system-view
[SW7750] vlan 2
```

Configure Ethernet2/0/1 port to be a Trunk port, with VLAN 6 as the default VLAN, and permit packets of VLAN 6 to pass through the port.

```
[SW7750-vlan2] quit
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] port link-type trunk
[SW7750-Ethernet2/0/1] port trunk pvid vlan 6
[SW7750-Ethernet2/0/1] port trunk permit vlan 6
```

Enable the voice VLAN feature on Ethernet 2/0/1, set the voice VLAN operation mode to **auto**, and bind VLAN 2 to Ethernet 2/0/1 as a voice VLAN.

```
[SW7750-Ethernet2/0/1] voice vlan enable
[SW7750-Ethernet2/0/1] voice vlan mode auto
[SW7750-Ethernet2/0/1] voice vlan 2
```

Voice VLAN Configuration Example (Manual Mode)

Network requirements

- Configure Ethernet2/0/3 port as a Trunk port for it to be added to/removed from the voice VLAN. Bind VLAN 2 to Ethernet 2/0/3 as a voice VLAN.
- Configure the OUI address to be 0011-2200-0000, with the description string being **test**.

Configuration procedure

Create VLAN 3.

```
<SW7750> system-view
[SW7750] vlan 3
[SW7750-vlan3] quit
```

Configure Ethernet2/0/3 port to be a Trunk port, specify VLAN 3 as its default VLAN, and permit packets of VLAN 3 to pass through the port.

```
[SW7750] interface Ethernet2/0/3
[SW7750-Ethernet2/0/3] port link-type trunk
[SW7750-Ethernet2/0/3] port trunk pvid vlan 3
[SW7750-Ethernet2/0/3] port trunk permit vlan 3
```

Enable voice VLAN on Ethernet 2/0/3, set the voice VLAN operation mode of Ethernet 2/0/3 to **manual**, and bind VLAN 3 to Ethernet 2/0/3 as a voice VLAN.

```
[SW7750-Ethernet2/0/3] voice vlan enable
[SW7750-Ethernet2/0/3] undo voice vlan mode auto
[SW7750-Ethernet2/0/3] voice vlan 3
```

Specify an OUI address.

```
[SW7750] voice vlan mac-address 0011-2200-0000 mask ffff-ff00-0000 d
escription test
```

Display voice VLAN-related configurations.

```
[SW7750] display voice vlan status
Voice Vlan security mode: Security
```

```
Voice Vlan aging time: 1440 minutes
Current voice vlan enabled port mode:
PORT                        MODE     STATUS             Voice Vlan ID
------------------------------------------------------------------------
Ethernet2/0/3               MANUAL   ENABLE               3
```

Remove Ethernet2/0/3 port from the voice VLAN.

```
[SW7750] interface Ethernet2/0/3
[SW7750-Ethernet2/0/3] undo port trunk permit vlan 3
```

13 ISOLATE-USER-VLAN CONFIGURATION

Isolate-User-VLAN Overview

Introduction to Isolate-User-VLAN

Isolate-user-VLAN is designed for saving VLAN resource by means of copying MAC address entries among the MAC address tables of VLANs in the network, which is utilizing the feature that an hybrid port removes the VLAN tag of packets coming from multiple VLANs.

Isolate-user-VLAN adopts Layer 2 VLAN structure, you need to configure two types of VLAN, isolate-user-VLAN and secondary VLAN.

An isolate-user-VLAN can match with multiple secondary VLANs. By setting the hybrid attribute for a port, ports included in all the secondary VLANs and the uplink port of a switch can all belong to an isolate-user-VLAN. At the same time, you should configure the uplink port to remove the VLAN tags of all the secondary VLAN packets forwarded by it.

In this case, for the upper layer switch, all the packets received from the lower stream are without VLAN tags. Therefore, the switch can reset the local VLAN structure to save VLAN resource without considering the VLAN configuration in the lower layer.

Isolate-User-VLAN Packets Forwarding Process

Figure 35 is the diagram for isolate-user-VLAN application, the following content describes the isolate-user-VLAN packets forwarding process based on this figure.

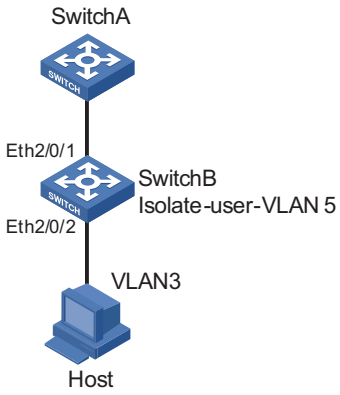
Configure Switch B

- Configure port Ethernet2/0/4 as a hybrid port, with the default VLAN ID being 3. At the same time, this port belongs to VLAN 3 and VLAN 5, and performs untag operation (removing of VLAN tag) on the packets from VLAN 3 and VLAN 5.
- Configure port Ethernet2/0/1 as a hybrid port, with the default VLAN ID being 5. At the same time, this port belongs to VLAN 3 and VLAN 5, and performs untag operation (removing of VLAN tag) on the packets from VLAN 3 and VLAN 5.

Configure Switch A

To ensure that packets sent by Switch A can be forwarded by Switch B according to the VLAN configurations of the lower layer devices, you need to configure the port through which Switch A connects to Switch B to remove VLAN tags when Switch A sends packets to Switch B.

Figure 35 Diagram for isolate-user-VLAN application



Forward packets to Switch A

1 When packets sent by PC reached Ethernet2/0/4, the default VLAN ID, that is, the VLAN tag of VLAN 3 is automatically added to the packets.

2 Switch B learns the MAC address of the PC, and adds it to the MAC address forwarding table of VLAN 3, and at the same time copies the entry to the MAC address forwarding table of VLAN 5.

3 Because Ethernet2/0/1 belongs to VLAN 3, the packets from VLAN 3 can pass through it, and Ethernet2/0/1 automatically removes the tag of VLAN 3, so that packets reaching Switch A is without the VLAN tag.

Receive and forward packets from Switch A

1 When packets coming from Switch A (the packets are configured to be without VLAN tag) reach to port Ethernet2/0/1 of Switch B, the packets are automatically added with default VLAN ID, that is, the tag of VLAN 5.

2 According to the MAC address forwarding table copied in the outbound process, the system will find the egress port being Ethernet2/0/4.

3 Because Ethernet2/0/4 belongs to VLAN 5, packets can pass through it normally, and at the same time, Ethernet2/0/4 removes the VLAN tag of the packets. So that the PC receives packets without VLAN tag.

Isolate-User-VLAN Configuration

Isolate-User-VLAN Configuration Tasks

Table 62 isolate-user-VLAN configuration tasks

Operation	Description	Related section
Configure isolate-user-VLAN	Required	"Configuring Isolate-User-VLAN" on page 115
Configure secondary VLAN	Required	"Configuring Secondary VLAN" on page 115
Add ports to isolate-user-VLAN and secondary VLAN and configure them to perform untag operation on packets	Required	"Adding Ports to isolate-user-VLAN and Secondary VLAN" on page 115

Table 62 isolate-user-VLAN configuration tasks

Operation	Description	Related section
Configure the mapping between the isolate-user-VLAN and the secondary VLAN	Required	"Configuring Mapping between isolate-user-VLAN and Secondary VLAN" on page 116

Configuring Isolate-User-VLAN

You can use the following commands to create an isolate-user-VLAN for a switch.

Table 63 Configure an isolate-user-VLAN

Operation	Command	Description
Enter system view	**system-view**	-
Create a VLAN and enter VLAN view	**vlan** *vlan-id*	Required
Set the VLAN type to isolate-user-VLAN	**isolate-user-vlan enable**	Required

CAUTION:

- *Multiple isolate-user-VLANs can be configured for a switch.*
- *With GVRP function enabled, a switch cannot be enabled with isolate-user-VLAN function.*
- *Isolate-user-VLAN does not forward multicast services data.*
- *The isolate-user-VLAN function and super VLAN function cannot be enabled simultaneously for a VLAN. If a VLAN is specified as an isolate-user-VLAN or a secondary VLAN, you cannot configure it as a super VLAN or a sub VLAN additionally.*

Configuring Secondary VLAN

Configuring a secondary VLAN is the same as configuring an ordinary VLAN.

Table 64 Configure secondary VLAN

Operation	Command	Description
Enter system view	**system-view**	-
Create a secondary VLAN	**vlan** *vlan-id*	Required

Adding Ports to isolate-user-VLAN and Secondary VLAN

In order to transmit packets normally, all ports included in the isolate-user-VLAN and the secondary VLAN must be hybrid ports, and all ports must perform untag operation on all VLAN packets.

Table 65 Add ports to isolate-user-VLAN and secondary VLAN and configure the ports to untagged packets

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Configure a port as a hybrid port	**port link-type hybrid**	Required

Table 65 Add ports to isolate-user-VLAN and secondary VLAN and configure the ports to untagged packets

Operation	Command	Description
Add a port to the isolate-user-VLAN and the secondary VLAN	**port hybrid vlan** *vlan-id* **untagged**	Required
Configure the default VLAN ID of a port	**port hybrid pvid vlan** *vlan-id*	Required

CAUTION: *When you use the* ***port hybrid pvid vlan*** *command to configure the default VLAN ID for a port, you need to specify the vlan-id as a secondary VLAN for a downlink port and specify the vlan-id an isolate-user-VLAN for an uplink port.*

Configuring Mapping between isolate-user-VLAN and Secondary VLAN

You can use the following command to establish the mapping relationship between an isolate-user-VLAN and a secondary VLAN.

Table 66 Configure isolate-user-VLAN-to-secondary VLAN mapping

Operation	Command	Description
Enter system view	**system-view**	-
Configure the mapping relationship between an isolate-user-VLAN and a secondary VLAN	**isolate-user-vlan** *vlan-id* **secondary** *vlan-list*	Required

CAUTION: *An isolate-user-VLAN can establish mapping relationship with multiple secondary VLANs, however, a secondary VLAN can establish mapping relationship with only one isolate-user-VLAN.*

Displaying Isolate-User-VLAN Configuration

After the above configurations, you can execute the display command in any view to view the running status of the isolate-user-VLAN and verify the configuration effect.

Table 67 Display isolate-user-VLAN configuration

Operation	Command	Description
Display the mapping relationship between the isolate-user-VLAN and the secondary VLAN	**display isolate-user-vlan** [*vlan-id*]	The **display** command can be executed in any view.

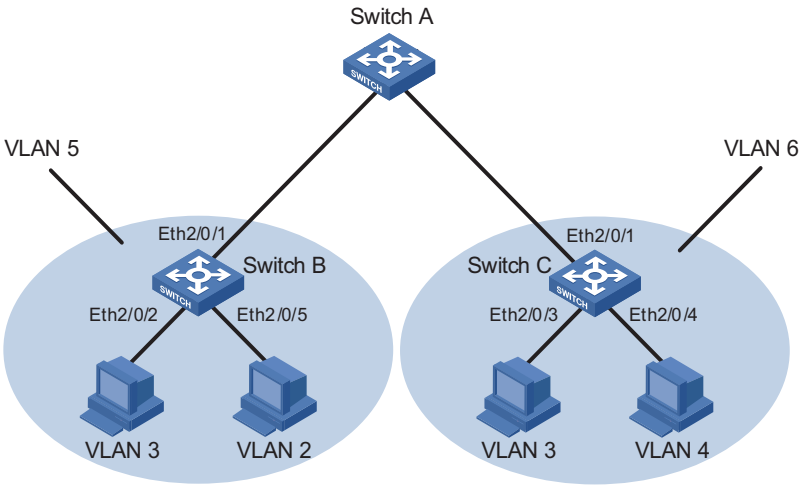
Isolate-User-VLAN Configuration Example

Network requirements

- Switch A connects with Switch B and Switch C. Packets from Switch B and Switch C to Switch A are without VLAN tag, so that Switch A needs not to consider the VLAN configurations of the lower layer switches.
- VLAN 5 on Switch B is an isolate-user-VLAN which includes the uplink port Ethernet2/0/1 and two secondary VLANs: VLAN 2 and VLAN 3. VLAN 3 includes port Ethernet2/0/2, and VLAN 2 includes port Ethernet2/0/5.
- VLAN 6 on Switch C is an isolate-user-VLAN which includes the uplink port Ethernet2/0/1 and two secondary VLANs: VLAN 3 and VLAN 4. VLAN 3 includes port Ethernet2/0/3, and VLAN 4 includes port Ethernet2/0/4.

Network diagram

Figure 36 Diagram for isolate-user-VLAN configuration



Configuration procedure

- Configure Switch B

Configure the isolate-user-VLAN

```
<SwitchB> system-view
[SwitchB] vlan 5
[SwitchB-vlan5] isolate-user-vlan enable
```

Configure the secondary VLAN.

```
[SwitchB-vlan5] quit
[SwitchB] vlan 3
[SwitchB-vlan3] quit
[SwitchB] vlan 2
```

Add port Ethernet2/0/2 to the isolate-user-VLAN and the secondary VLAN, and configure the port to untag the VLAN packets. Because all ports are added to VLAN 1 by default, you need to remove the port from VLAN 1 to avoid broadcast.

```
[SwitchB-vlan2] quit
[SwitchB] interface Ethernet 2/0/2
[SwitchB-Ethernet2/0/2] port link-type hybrid
[SwitchB-Ethernet2/0/2] port hybrid vlan 3 untagged
[SwitchB-Ethernet2/0/2] port hybrid vlan 5 untagged
[SwitchB-Ethernet2/0/2] port hybrid pvid vlan 3
[SwitchB-Ethernet2/0/2] undo port hybrid vlan 1
```

Add port Ethernet2/0/5 to the isolate-user-VLAN and the secondary VLAN, and configure the port to untag the VLAN packets. Remove the port from VLAN 1.

```
[SwitchB-Ethernet2/0/2] quit
[SwitchB] interface Ethernet 2/0/5
[SwitchB-Ethernet2/0/5] port link-type hybrid
[SwitchB-Ethernet2/0/5] port hybrid vlan 2 untagged
[SwitchB-Ethernet2/0/5] port hybrid vlan 5 untagged
```

```
[SwitchB-Ethernet2/0/5] port hybrid pvid vlan 2
[SwitchB-Ethernet2/0/5] undo port hybrid vlan 1
```

Add port Ethernet2/0/1 to the isolate-user-VLAN and the secondary VLAN, and configure the port to untag the VLAN packets. Remove the port from VLAN 1.

```
[SwitchB-Ethernet2/0/5] quit
[SwitchB] interface Ethernet 2/0/1
[SwitchB-Ethernet2/0/1] port link-type hybrid
[SwitchB-Ethernet2/0/1] port hybrid vlan 2 untagged
[SwitchB-Ethernet2/0/1] port hybrid vlan 3 untagged
[SwitchB-Ethernet2/0/1] port hybrid vlan 5 untagged
[SwitchB-Ethernet2/0/1] port hybrid pvid vlan 5
[SwitchB-Ethernet2/0/1] undo port hybrid vlan 1
```

Configure isolate-user-VLAN-to-secondary VLAN mapping.

```
[SwitchB-Ethernet2/0/1] quit
[SwitchB] isolate-user-vlan 5 secondary 2 to 3
```

- Configure Switch C

Configure the isolate-user-VLAN

```
<SwitchC> system-view
[SwitchC] vlan 6
[SwitchC-vlan6] isolate-user-vlan enable
```

Configure the secondary VLAN.

```
[SwitchC-vlan6] quit
[SwitchC] vlan 3
[SwitchC-vlan3] vlan 4
```

Add port Ethernet2/0/3 to the isolate-user-VLAN and the secondary VLAN, and configure the port to untag the VLAN packets. Remove the port from VLAN 1.

```
[SwitchC-vlan4] quit
[SwitchC] interface Ethernet 2/0/3
[SwitchC-Ethernet2/0/3] port link-type hybrid
[SwitchC-Ethernet2/0/3] port hybrid vlan 3 untagged
[SwitchC-Ethernet2/0/3] port hybrid vlan 6 untagged
[SwitchC-Ethernet2/0/3] port hybrid pvid vlan 3
[SwitchB-Ethernet2/0/3] undo port hybrid vlan 1
```

Add port Ethernet2/0/4 to the isolate-user-VLAN and the secondary VLAN, and configure the port to untag the VLAN packets. Remove the port from VLAN 1.

```
[SwitchC-Ethernet2/0/3] quit
[SwitchC] interface Ethernet2/0/4
[SwitchC-Ethernet2/0/4] port link-type hybrid
[SwitchC-Ethernet2/0/4] port hybrid vlan 4 untagged
[SwitchC-Ethernet2/0/4] port hybrid vlan 6 untagged
[SwitchC-Ethernet2/0/4] port hybrid pvid vlan 4
[SwitchB-Ethernet2/0/4] undo port hybrid vlan 1
```

Add port Ethernet2/0/1 to the isolate-user-VLAN and the secondary VLAN, and configure the port to untag the VLAN packets. Remove the port from VLAN 1.

```
[SwitchC-Ethernet2/0/4] quit
[SwitchC] interface Ethernet 2/0/1
[SwitchC-Ethernet2/0/1] port link-type hybrid
[SwitchC-Ethernet2/0/1] port hybrid vlan 3 untagged
[SwitchC-Ethernet2/0/1] port hybrid vlan 4 untagged
[SwitchC-Ethernet2/0/1] port hybrid vlan 6 untagged
[SwitchC-Ethernet2/0/1] port hybrid pvid vlan 6
[SwitchB-Ethernet2/0/1] undo port hybrid vlan 1
```

Configure isolate-user-VLAN-to-secondary VLAN mapping.

```
[SwitchC-Ethernet2/0/1] quit
[SwitchC] isolate-user-vlan 6 secondary 3 to 4
```

After the above configurations, Switch A can receive packets from Switch B and Switch C, and they are all packets without VLAN tag. Each VLAN 3 configured on Switch B and Switch C cannot communicate with each other because the packets from them are stripped off the original VLAN tags before reaching Switch A and then be encapsulated with the VLAN tag set on Switch A. This makes the lower switches only own locally valid VLAN configuration. And in this way, the global VLAN resource is saved.

14 SUPER VLAN

Only the 96Gbps switch fabrics support the super VLAN.

Super VLAN Overview

To save IP address resources, the super VLAN concept (also known as VLAN aggregation) was developed. Its principle is like this: a super VLAN may include multiple sub VLANs, with each as a broadcast domain. Layer 2 isolation is implemented between sub VLANs. The super VLAN can be configured with a Layer 3 interface, but not the sub VLAN.

When users in different sub VLANs want Layer 3 communication, they use the IP address of the Layer 3 interface of the super VLAN as their gateway address. IP address resources are saved since multiple sub VLANs share one IP address.

At the same time, in order to realize the Layer 3 connectivity between the sub VLANs and between the sub VLAN and other networks, ARP proxy function is used. ARP proxy enables Layer 3 connectivity between Layer 2 isolated ports by performing ARP request and forwarding and handling response packets.

Super VLAN Configuration

Super VLAN Configuration Tasks

Table 68 Super VLAN configuration tasks

Operation	Description	Related section
Configure a super VLAN	Optional	"Configuring a Super VLAN" on page 121
Configure a sub VLAN	Optional	"Configuring a Sub VLAN" on page 122
Configure the mapping between super VLAN and sub VLAN	Optional	"Configuring the Mapping between a Super VLAN and a Sub VLAN" on page 122
Configure super VLAN to support DHCP relay	Optional	"Configuring Super VLAN to Support DHCP Relay" on page 123

Configuring a Super VLAN

You can configure multiple super VLANs for a switch. You can use the following commands to specify a VLAN as a super VLAN. After a VLAN is configured as a super VLAN, the configuration of corresponding VLAN interfaces and IP addresses is the same as the configuration for an ordinary VLAN.

Table 69 Configure a VLAN as a super VLAN

Operation	Command	Description
Enter system view	**system-view**	-
Enter VLAN view	**vlan** *vlan-id*	-
Configure the current VLAN as a super VLAN	**supervlan**	Required

CAUTION: *You can not configure a VLAN which includes Ethernet ports as a super VLAN; and after you configure a super VLAN, you cannot add any Ethernet port to it.*

Configuring a Sub VLAN

You can configure a sub VLAN just as configuring an ordinary VLAN. See "VLAN Configuration" on page 95 for details. The configuration commands are shown in the following table.

Table 70 Configure a sub VLAN

Operation	Command	Description
Enter system view	**system-view**	-
Create a sub VLAN	**vlan** *vlan-id*	Required
Add an Ethernet port to the sub VLAN	**port** *interface-list*	Required

CAUTION: *The **port** command is only used to add the access port to a sub VLAN. If you want to add a trunk port or a hybrid port to a sub VLAN, you must execute the **port trunk permit vlan** command and the **port hybrid vlan** command in Ethernet port view. Refer to "Configuring a Trunk-Port-Based VLAN" on page 98 and "Configuring a Hybrid-Port-Based VLAN" on page 98.*

Note that you can add multiple ports (except the uplink port) for a sub VLAN.

Configuring the Mapping between a Super VLAN and a Sub VLAN

You can use the following commands to establish the mapping between a super VLAN and a sub VLAN.

Table 71 Configure the mapping between a super VLAN and a sub VLAN

Operation	Command	Description
Enter system view	**system-view**	-
Enter VLAN view of the super VLAN	**vlan** *vlan-id*	-
Establish the mapping between a super VLAN and a sub VLAN	**port** *interface-list*	Required

CAUTION:

- *The sub VLAN must exist before you create mapping between the sub VLAN and the super VLAN.*
- *When you establish mapping between the super VLAN and the sub VLAN, if a VLAN interface is configured for the sub VLAN, the system will prompt you to delete the interface to establish the mapping successfully.*

- *After establishing the mapping between the sub VLAN and the super VLAN, you can still add (or delete) ports to (from) the sub VLAN.*

Configuring Super VLAN to Support DHCP Relay

With DHCP relay function enabled on the VLAN interface of the super VLAN, the hosts of all sub VLANs that map with the super VLAN can dynamically obtain IP addresses from the outside networks.

With the DHCP relay function enabled on the VLAN interface of the super VLAN, the host of the sub VLAN that maps the interface and the DHCP host in another network segment can forward the DHCP packets to each other, so as to assist the hosts in the sub VLANs to finish the dynamic configuration of IP address.

Configuration Prerequisites

- Configure a super VLAN and a sub VLAN, and establish the mapping between them.
- Configure the IP address of the super VLAN to make the hosts in the sub VLAN being able to communicate with the outside network.

Configuration Procedure

Operation	Command	Description
Enter system view	**system-view**	-
Enter VLAN interface view of the super VLAN	**interface Vlan-interface** *vlan-id*	-
Configure the mapping between the interface and the DHCP server group	**dhcp-server** *groupNo*	Required By default, the VLAN interface does not establish homing relationship with any DHCP server group.

- *A super VLAN interface can only correspond to one DHCP server group.*
- *The last configuration will take effect if you execute the **dhcp-server** groupNo command.*
- *The group number specified in the **dhcp-server** groupNo command needs to be configured first in the **dhcp-server ip** command. Refer to "Configuring an Interface to Operate in DHCP Relay Agent Mode" on page 614.*

Displaying Super VLAN

After the above configurations, you can use the **display** command in any view the super VLAN configuration and verify the configuration effect.

Table 72 Display super VLAN configuration

Operation	Command	Description
Display the mapping between the super VLAN and the sub VLAN	**display supervlan** [*supervlan-id*]	The **display** command can be executed in any view.

Super VLAN Configuration Example

Super VLAN Configuration Example

Network Requirements

- Create super VLAN 10 and sub VLANs VLAN 2, VLAN 3, VLAN 5.
- Configure ports Ethernet2/0/1 and Ethernet2/0/2 to belong to VLAN 2, Ethernet2/0/3 and Ethernet2/0/4 to belong to VLAN 3 and Ethernet2/0/5 and Ethernet2/0/6 to belong to VLAN 5.
- Configure Layer 3 connectivity between sub VLANs, and all sub VLANs use the Layer 3 interface of the super VLAN (with the IP address being 10.110.1.1) as the gateway to communicate with the outside.

Network diagram

Omitted

Configuration procedure

Create VLAN 10, and enable the super VLAN function on it.

```
<SW7750> system-view
[SW7750] vlan 10
[SW7750-vlan10] supervlan
```

Create VLAN2, VLAN3, and VLAN5, and add corresponding ports to them.

```
[SW7750-vlan10] quit
[SW7750] vlan 2
[SW7750-vlan2] port Ethernet 2/0/1 Ethernet 2/0/2
[SW7750-vlan2] quit
[SW7750] vlan 3
[SW7750-vlan3] port Ethernet 2/0/3 Ethernet 2/0/4
[SW7750-vlan3] quit
[SW7750] vlan 5
[SW7750-vlan5] port Ethernet 2/0/5 Ethernet 2/0/6
```

Configure the mapping between the super VLAN and the sub VLAN.

```
[SW7750-vlan5] quit
[SW7750] vlan 10
[SW7750-vlan10] subvlan 2 3 5
```

Create the Layer 3 interface of the super VLAN, and configure an IP address for it.

```
[SW7750-vlan10] quit
[SW7750] interface Vlan-interface 10
[SW7750-Vlan-interface10] ip address 10.110.1.1 255.255.255.0
```

Super VLAN Supporting DHCP Relay Example

Network requirements

- Create VLAN 6 as a super VLAN, and create VLAN 2 and VLAN 3 as the sub VLANs which map VLAN 6.

- Configure the IP address of the VLAN 6 as 10.1.1.1, and the sub network mask as 255.255.255.0.
- Enable the DHCP relay function on the VLAN interface of VLAN 6, and establish the mapping between VLAN 6 and the remote DHCP server group 2 to make the hosts in VLAN 2 and VLAN 3 being able to dynamically obtain IP addresses from the DHCP server group 2.

Configuration Procedure

Create VLAN 6, and configure it as a super VLAN.

```
<SW7750> system-view
[SW7750] vlan 6
[SW7750-vlan6] supervlan
```

Create VLAN 2 and VLAN 3 and establish the mapping between them and VLAN 6.

```
[SW7750-vlan6] quit
[SW7750] vlan 2
[SW7750-vlan2] quit
[SW7750] vlan 3
[SW7750-vlan3] quit
[SW7750] vlan 6
[SW7750-vlan6] subvlan 2 3
```

Create the VLAN interface of VLAN 6, and configure an IP address for it.

```
[SW7750-vlan6] quit
[SW7750] interface Vlan-interface 6
[SW7750-Vlan-interface6] ip address 10.1.1.1 255.255.255.0
```

Enable the DHCP relay function on the VLAN 6 interface, that is, establish the mapping between the interface and the DHCP server group 2.

```
[SW7750-Vlan-interface6] dhcp-server 2
```

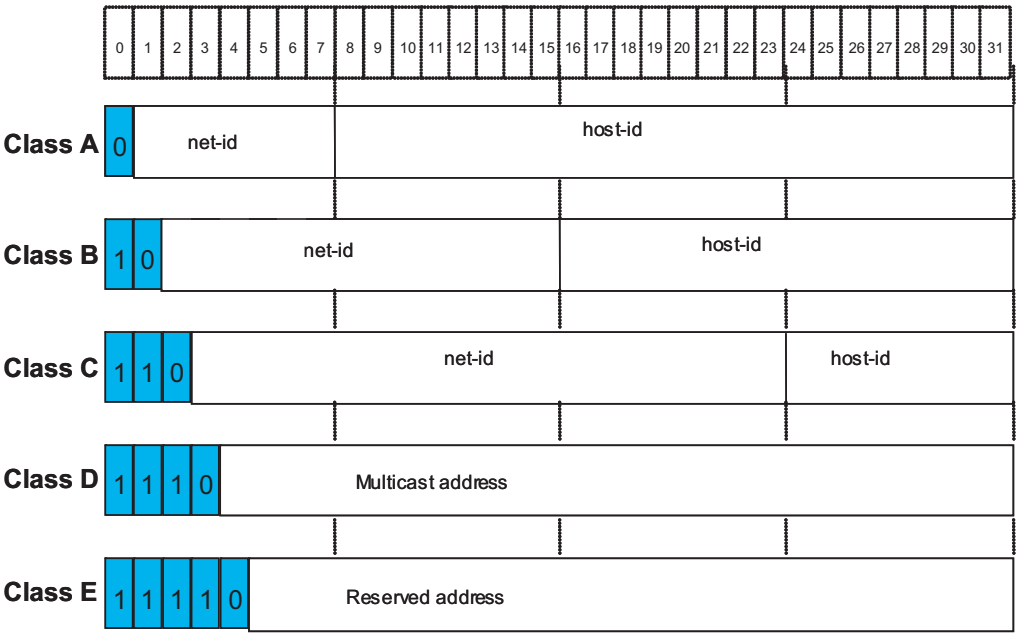
15 IP ADDRESS CONFIGURATION

IP Address Overview

IP Address Classification and Representation

An IP address is a 32-bit address allocated to a device connected to the Internet. It consists of two fields: net-id and host-id. To facilitate IP address management, IP addresses are divided into five classes, as shown in Figure 37.

Figure 37 Five classes of IP addresses



net-id: Network ID; host-id: Host ID

Class A, Class B, and Class C IP addresses are unicast addresses. Class D IP addresses are multicast addresses and Class E addresses are reserved for future special use. The first three types are commonly used.

IP addresses are in the dotted decimal notation. Each IP address contains four decimal integers, with each integer corresponding to one byte (for example,10.110.50.101).

Some IP addresses are reserved for special use. The IP address ranges that can be used by users are listed in Table 73.

Table 73 Classes and ranges of IP addresses

Network type	Address range	IP network range	Description
A	0.0.0.0 to 127.255.255.255	1.0.0.0 to 126.0.0.0	■ An IP address with all 0s host ID is a network address and is used for network routing. ■ An IP address with all 1s host ID is a broadcast address and is used for broadcast to all hosts on the network. ■ The IP address 0.0.0.0 is used by hosts when they are booted but is not used afterward. ■ An IP address with all 0s network ID represents a specific host on the local network and can be used as a source address but cannot be used as a destination address. ■ All the IP addresses in the format of 127.X.Y.Z are reserved for loopback test and the packets sent to these addresses will not be output to lines; instead, they are processed internally and regarded as incoming packets.
B	128.0.0.0 to 191.255.255.255	128.0.0.0 to 191.255.0.0	■ An IP address with all 0s host ID is a network address and is used for network routing. ■ An IP address with all 1s host ID is a broadcast address and is used for broadcast to all hosts on the network.
C	192.0.0.0 to 223.255.255.255	192.0.0.0 to 223.255.255.0	■ An IP address with all 0s host ID is a network address and is used for network routing. ■ An IP address with all 1s host ID is a broadcast address and is used for broadcast to all hosts on the network.
D	224.0.0.0 to 239.255.255.255	None	Class D addresses are multicast addresses.
E	240.0.0.0 to 255.255.255.254	None	These IP addresses are reserved for future use.
Others	255.255.255.255	255.255.255.255	255.255.255.255 is used as a LAN broadcast address.

Subnet and Mask

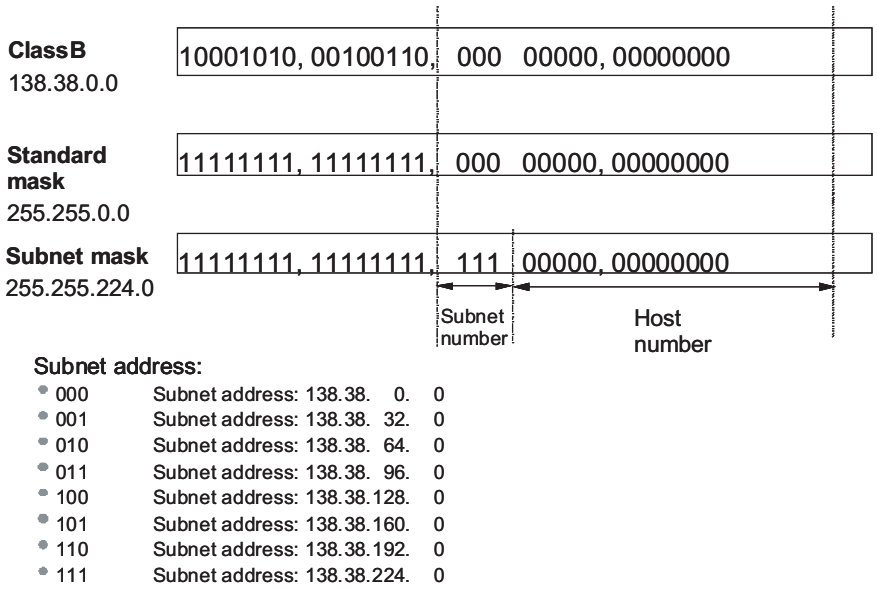
The traditional IP address classification method wastes IP addresses greatly. In order to make full use of the available IP addresses, the concepts of mask and subnet were introduced.

A mask is a 32-bit number corresponding to an IP address. The number consists of 1s and 0s. A mask is defined as follows: the bits of the network number and subnet number are set to 1, and the bits of the host number are set to 0. The mask divides the IP address into two parts: subnet address and host address. In an IP address, the part corresponding to the "1" bits in the mask is the subnet

address, and the part corresponding to the remaining "0" bits in the mask is the host address. If there is no subnet division, the subnet mask uses the default value and the length of 1s in the mask is equal to the net-id length. Therefore, for IP addresses of classes A, B and C, the default values of the corresponding subnet masks are 255.0.0.0, 255.255.0.0 and 255.255.255.0 respectively.

The mask can be used to divide a Class A network containing more than 16,000,000 hosts or a Class B network containing more than 60,000 hosts into multiple small networks. Each small network is called a subnet. For example, for the Class B network address 138.38.0.0, the mask 255.255.224.0 can be used to divide the network into eight subnets: 138.38.0.0, 138.38.32.0, 138.38.64.0, 138.38.96.0, 138.38.128.0, 138.38.160.0, 138.38.192.0 and 138.38.224.0 (see Figure 38). Each subnet can contain more than 8000 hosts.

Figure 38 Subnet division of the IP address



Configuring an IP Address for a VLAN Interface

A VLAN interface obtains an IP address with an IP address configuration command. Generally, it is enough to configure one IP address for a VLAN interface. However, you can configure up to eight IP addresses for a VLAN interface so that the interface can be connected to several subnets. Among these IP addresses, one is the primary IP address and the others are secondary ones.

Table 74 Configure an IP address for a VLAN interface

Operation	Command	Description
Enter system view	**system-view**	-
Enter VLAN interface view	**interface Vlan-interface** *vlan-id*	-
Configure an IP address for a VLAN interface	**ip address** *ip-address* { *mask* | *mask-length* } [**sub**]	Required By default, a VLAN interface has no IP address.

Displaying IP Address Configuration

After the above configuration, you can execute the **display** command in any view to display the operating status and configuration on the interface to verify your configuration.

Table 75 Display IP address configuration

Operation	Command	Description
Display VLAN interface information	**display ip interface** [**brief**] [*interface-type interface-number*]	You can execute the **display** command in any view

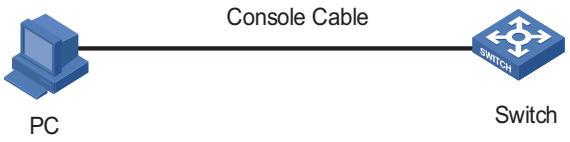
IP Address Configuration Example

Network requirements

Set the IP address and subnet mask of VLAN interface 1 to 129.2.2.1 and 255.255.255.0 respectively.

Network diagram

Figure 39 IP address configuration



Configuration procedure

Configure an IP address for VLAN interface 1.

```
<Switch> system-view
[Switch] interface Vlan-interface 1
[Switch-Vlan-interface1] ip address 129.2.2.1 255.255.255.0
```

Troubleshooting

Symptom: The switch cannot ping the host directly-connected to a port.

Solution: You can perform troubleshooting as follows:

- Check the configuration of the switch, and then use the **display arp** command to check whether the host has an corresponding ARP entry in the ARP table maintained by the Switch.
- Check the VLAN that includes the switch port connecting the host. Check whether the VLAN has been configured with the VLAN interface. Then check whether the IP addresses of the VLAN interface and the host are on the same network segment.
- If the configuration is correct, enable ARP debugging on the switch, and check whether the switch can correctly send and receive ARP packets. If it can only send but cannot receive ARP packets, errors may occur at the Ethernet physical layer.

16 IP PERFORMANCE CONFIGURATION

IP Performance Overview

Introduction to TCP Attributes

IP performance configuration mainly refers to TCP attribute configuration. The TCP attributes that can be configured include:

- synwait timer: This timer is started when TCP sends a syn packet. If no response packet is received before the timer times out, the TCP connection will be terminated. The timeout of the synwait timer ranges from 2 to 600 seconds and is 75 seconds by default.
- finwait timer: This timer is started when the TCP connection turns from the FIN_WAIT_1 state to the FIN_WAIT_2 state. If no FIN packet is received before the timer times out, the TCP connection will be terminated. The timeout of the finwait timer ranges from 76 to 3,600 seconds and is 675 seconds by default.
- The connection-oriented socket receive/send buffer size ranges from 1 to 32 KB and is 8 KB by default.

Introduction to FIB

Every switch stores a forwarding information base (FIB). FIB is used to store the forwarding information of the switch and guide Layer 3 packet forwarding.

You can know the forwarding information of the switch through the FIB table. Each FIB entry includes: destination address/mask length, next hop, current flag, timestamp, and outbound interface.

When the switch is running normally, the contents of the FIB and the routing table are the same. For routing and routing tables, refer to "Routing Table" on page 281.

IP Performance Configuration

Table 76 Configure IP

Configuration task	Description	Detailed configuration
Configure TCP attributes	Required	"Configuring TCP Attributes" on page 132
Configure to send special IP packets to CPU	Required	"Configuring to Send Special IP Packets to CPU" on page 132
Enable forwarding of directed broadcasts to a directly connected network	Required	"Enabling Forwarding of Directed Broadcasts to a Directly Connected Network" on page 132
Disable ICMP error message sending	Required	"Disabling ICMP Error Message Sending" on page 133

Configuring TCP Attributes

Table 77 Configure TCP attributes

Operation	Command	Description
Enter system view	**system-view**	-
Configure timeout time for the synwait timer in TCP	**tcp timer syn-timeout** *time-value*	Required The default value is 75 seconds
Configure timeout time for the finwait timer in TCP	**tcp timer fin-timeout** *time-value*	Required The default value is 675 seconds
Configure the socket receiving and sending buffer size of TCP	**tcp window** *window-size*	Required By default, the size of the socket receiving and sending buffers is 8 KB

Configuring to Send Special IP Packets to CPU

Usually the switch sends TTL timeout packets and unreachable packets to the CPU in the process of forwarding IP packets. The CPU processes these special packets after receiving them. Incorrect configuration and malicious attack will cause heavy CPU load. You can perform the following configuration to configure not to send corresponding packets to the CPU in order to ensure normal running.

Table 78 Configure to send special IP packets to CPU

Operation	Command	Description
Enter system view	**system-view**	-
Configure to send TTL timeout packets and unreachable packets to CPU	**ip** { **ttl-expires** | **unreachables** }	Required By default, unreachable packets are not sent to the CPU, while TTL timeout packets are sent to the CPU

Enabling Forwarding of Directed Broadcasts to a Directly Connected Network

Broadcast packets include full-net broadcast packets and directed broadcast packets. The destination IP address of a full-net broadcast packet is all 1s (255.255.255.255). A directed broadcast packet is a packet whose destination IP address is the network broadcast address of a subnet, but the source IP address is not in the subnet. When a switch forwards a directed broadcast packet, it cannot tell whether the packet is a broadcast packet if the switch is not connected with the subnet.

If a directed broadcast packet reaches the destination network after being forwarded by the switch, the switch will receive the broadcast packet, for the switch also belongs to the subnet. Since the VLAN of the switch isolates the broadcast domain, the switch will stop forwarding the packet to the network. Using the commands, you can choose to forward the directed broadcast packet to the directly connected network.

If you reference an ACL to filter directed broadcasts, only the directed broadcasts that pass the ACL filtering can be forwarded to the directly connected network.

Table 79 Enable forwarding of directed broadcast packets

Operation	Command	Description
Enter system view	**system-view**	-
Enter VLAN interface view	**interface** *interface-type interface-number*	-
Enable forwarding of directed broadcast packets to a directly connected network	**ip forward-broadcast** [*acl-number*]	Required By default, the switch does not forward directed broadcast packets to a directly connected network.

Disabling ICMP Error Message Sending

Sending error packets is the major function of the Internet Control Message Protocol (ICMP). ICMP packets are usually sent by the network layer protocols or transport layer protocols to notify corresponding devices of failures.

Although sending ICMP error packets facilitates network control and management, it still has the following disadvantages:

- Sending a lot of ICMP packets will increase network traffic.
- If receiving a lot of malicious packets that cause a device to send ICMP error packets, the device's performance will be reduced.
- As the ICMP redirection function increases the routing table size of hosts, the hosts' performance will be reduced if the routing table becomes very large.
- If a host sends malicious ICMP destination unreachable packets, end users may be affected.

To solve such problems, you can disable a device from sending ICMP error packets.

Currently, you can only disable the sending of ICMP redirect messages.

Table 80 Disable ICMP redirect message sending

Operation	Command	Description
Enter system view	**system-view**	-
Disable ICMP redirect message sending	**undo icmp redirect send**	Required By default, the ICMP redirect message sending is enabled.

Displaying and Debugging IP Performance

After the above configurations, you can execute the **display** command in any view to display the running status to verify your IP performance configuration.

Table 81 Display IP performance

Operation	Command	Description
Display TCP connection status	**display tcp status**	You can execute the **display** command in any view.
Display TCP connection statistics	**display tcp statistics**	
Display UDP traffic statistics	**display udp statistics**	
Display IP traffic statistics	**display ip statistics**	
Display ICMP traffic statistics	**display icmp statistics**	
Display the current socket information of the system	**display ip socket** [**socktype** *sock-type*] [*task-id socket-id*]	
Display the summary of the forwarding information base (FIB) entry matching the specified rule	**display fib** *fib-rule*	

Use the **reset** command in user view to clear the IP, TCP, and UDP traffic statistics.

Table 82 Debug IP performance

Configuration	Command	Description
Clear IP traffic statistics	**reset ip statistics**	The **reset** command can be executed in user view
Clear TCP traffic statistics	**reset tcp statistics**	
Clear UDP traffic statistics	**reset udp statistics**	

Troubleshooting

Symptom: IP packets are forwarded normally, but TCP and UDP cannot work normally.

Solution: Enable the corresponding debugging information output to view the debugging information.

- Use the **display** command to display the IP performance and check whether the PC runs normally.
- Use the **terminal debugging** command to enable debugging information to be output to the console.
- Use the **debugging udp packet** command to enable the UDP debugging to trace UDP packets.

```
<Switch> terminal debugging
<Switch> debugging udp packet
```

The UDP packets are shown in the following format:

```
UDP output packet:
Source IP address:202.38.160.1
Source port:1024
Destination IP Address 202.38.160.1
Destination port: 4296
```

- Use the **debugging tcp packet** command to enable the TCP debugging to trace TCP packets.

```
<Switch> terminal debugging
<Switch> debugging tcp packet
```

Then the TCP packets received or sent will be displayed in the following format in real time:

```
TCP output packet:
Source IP address:202.38.160.1
Source port:1024
Destination IP Address 202.38.160.1
Destination port: 4296
Sequence number :4185089
Ack number: 0
Flag  :SYN
Packet length :60
Data offset: 10
```

17 IPX CONFIGURATION

IPX Protocol Overview

The Internetwork packet exchange (IPX) protocol is a network layer protocol in the NetWare protocol suite. IPX's position in the Novell Netware protocol is similar to IP's in the TCP/IP protocol suite. IPX can address, route and forward packets.

IPX is a connectionless protocol. Though an IPX packet includes a destination IPX address in addition to the data, there is no guarantee of successful delivery. Packet acknowledgement and connection control must be provided by protocols above IPX. In IPX, each IPX packet is considered as an independent entity that has no logical or sequential relationship with any other IPX packets.

IPX Address Structure

IPX and IP use different address structures. An IPX address comprises two parts: the network number and the node address; it is in the format of network.node.

A network number identifies the network where a site is located. It is four bytes long and expressed by eight hexadecimal numbers. A node address identifies a node on the network. Like a MAC address, it is six bytes long and written with the bytes being separated into three 2-byte parts by "-". The node address cannot be a broadcast or multicast address. For example, in the IPX address bc.0-0cb-47, bc (or 000000bc) is the network number and 0-0cb-47 (0000-00cb-0047) is the node address. You can also write an IPX address in the form of N.H-H-H, where N is the network number and H-H-H is the node address.

Routing Information Protocol

IPX uses the routing information protocol (RIP) to maintain and advertise dynamic routing information. With IPX enabled, the switch exchanges routing information with other neighbors through RIP to maintain an internetwork routing information database (also known as a routing table) to accommodate to the network changes. When the switch receives a packet, it looks up the routing table for the next site and if there is any, and then forwards the packet. The routing information can be configured statically or collected dynamically.

This chapter introduces RIP in IPX. For the RIP configurations on an IP network, refer to "Basic RIP Configuration" on page 291.

Service Advertising Protocol

IPX uses the service advertising protocol (SAP) to maintain and advertise dynamic service information. SAP advertises the services provided by servers and their addresses as well. With SAP, a server broadcasts its services when it starts up and the termination of the services when it goes down.

With IPX enabled, the switch creates and maintains an internetwork service information database (or the service information table) through SAP. It helps you learn what services are available on the networks and where they are provided. The servers periodically broadcast their services and addresses to the networks

directly connected to them. However, you cannot use such information directly. Instead, the information is collected by the SAP agents of the switches on the networks and saved in their server information tables.

IPX Configuration

Configuring IPX

Table 83 Configure IPX

Configuration task	Description	Detailed configuration
Basic IPX configuration	Required	"Basic IPX Configuration" on page 138
IPX routing configuration	Required	"Configuring IPX Routing" on page 138
IPX RIP configuration	Required	"Configuring IPX RIP" on page 139
IPX SAP configuration	Required	"Configuring IPX SAP" on page 141
IPX forwarding-related configuration	Required	"Configuring IPX forwarding" on page 144

Basic IPX Configuration

Table 84 Basic IPX configuration

Operation	Command	Description
Enter system view	**system-view**	-
Enable IPX	**ipx enable**	Required IPX is disabled by default
Enter VLAN interface view	**interface Vlan-interface** *vlan-id*	-
Configure an IPX network number for the VLAN interface	**ipx network** *network*	Required By default, the system does not assign network numbers to VLAN interface. That is, IPX is disabled on all the VLAN interfaces



- *After the **undo ipx enable** command is executed, the IPX configurations are cannot be recovered with the **ipx enable** command.*
- *After IPX is enabled, you must assign a network number to a VLAN interface to enable IPX on this VLAN interface. One network number can be assigned to only one VLAN interface.*
- *If the IPX network number of a VLAN interface is deleted, the IPX configuration and static routing information of this VLAN interface will be deleted at the same time.*

Configuring IPX Routing

Configuring IPX static routes

Table 85 Configure IPX static routes

Operation	Command	Description
Enter system view	**system-view**	-

Table 85 Configure IPX static routes

Operation	Command	Description
Enable IPX	**ipx enable**	Required IPX is disabled by default
Enter VLAN interface view	**interface Vlan-interface** *vlan-id*	-
Configure an IPX network number for the VLAN interface	**ipx network** *network*	Required By default, the system does not assign network numbers to VLAN interface. That is, IPX is disabled on all the VLAN interfaces
Exit VLAN interface view	**quit**	-
Configure IPX static routes	**ipx route-static** *network network.node* [**preference** *value*] [**tick** *ticks* **hop** *hops*]	Optional The IPX static routes whose destination network number is 0xFFFFFFFE are default routes

Configuring an IPX route limit

In IPX, you can configure in the routing table the maximum number of the dynamic routes and equivalent routes to the same destination. These two limit settings are independent.

When the number of the dynamic routes to the same destination address exceeds the limit, new dynamic routes are dropped directly without being added into the routing table. When the new setting is smaller than the old value, the switch, however, does not delete the excessive route entries. These route entries age out automatically.

If the new limit is smaller than the current active route number, the system deactivates the excessive active routes. If the new limit is greater than the number of current active routes, the system activates the equivalent routes that are available for them until the limit is reached.

Table 86 Configure an IPX route limit

Operation	Command	Description
Enter system view	**system-view**	-
Enable IPX	**ipx enable**	Required IPX is disabled by default
Configure the maximum number of dynamic routes to the same destination	**ipx route max-reserve-path** *paths*	Optional By default, the maximum number of dynamic routes to the same destination is 4
Configure the maximum number of equivalent routes to the same destination	**ipx route load-balance-path** *paths*	Optional By default, the maximum number of equivalent routes to the same destination is 1

Configuring IPX RIP

After IPX is enabled on VLAN interfaces, the system automatically enables RIP. You can configure IPX RIP parameters as needed.

Table 87 Configure IPX RIP

Operation	Command	Description
Enter system view	**system-view**	-
Enable IPX	**ipx enable**	Required IPX is disabled by default
Configure the update interval of IPX RIP	**ipx rip timer update seconds**	Optional By default, the update interval of IPX RIP is 60 seconds
Configure the aging period of IPX RIP	**ipx rip multiplier multiplier**	Optional By default, the aging period is three times the RIP updating interval
Configure IPX RIP to import static routes	**ipx rip import-route static**	Optional By default, IPX RIP does not import static routes.
Enter VLAN interface view	**interface Vlan-interface vlan-id**	-
Configure an IPX network number for the VLAN interface	**ipx network network**	Required By default, the system does not assign network numbers to VLAN interface. That is, IPX is disabled on all the VLAN interfaces
Configure the size of IPX RIP update packets	**ipx rip mtu bytes**	Optional By default, the maximum size of IPX RIP update packets is 432 bytes
Configure the IPX packet forwarding delay on a VLAN interface	**ipx tick ticks**	Optional By default, the forwarding delay on the VLAN interface is one tick

After IPX RIP is enabled, the switch broadcasts IPX RIP update packets periodically. You can configure the update interval of IPX RIP as required. Note that for the synchronization of routing tables, all the switches on the network must have the same RIP update interval.

The aging period of IPX RIP is a multiple of the IPX RIP update interval. You can set multiple update intervals as an aging period. If a routing entry is not updated after three RIP update intervals, it will be deleted from the routing table. At the same time, its associated dynamic service entry will be deleted from the service information table.

By default, the maximum IPX RIP update packet size is 432 bytes. Considering the 32 bytes for the IPX and RIP headers, each update packet can carry up to 50 eight-byte routing entries.

IPX RIP uses hop count and ticks to measure the distance to a destination network and route packets. The hop count of a packet adds by one upon each forwarding. Ticks (1 tick = 1/18 seconds) indicate the delay that a VLAN interface experiences

to forward an IPX packet. A longer delay means slower forwarding whereas a shorter delay means faster forwarding.

By importing routes, different routing protocols can share their routing information. Note that IPX RIP imports only active static routes; inactive static routes are neither imported nor forwarded.

Configuring IPX SAP

Enabling IPX SAP

After IPX is enabled on VLAN interfaces, the system enables SAP automatically. You can configure SAP parameters and service information as needed.

Table 88 Configure IPX SAP

Operation	Command	Description
Enter system view	**system-view**	-
Enable IPX	**ipx enable**	Required IPX is disabled by default
Enter VLAN interface view	**interface Vlan-interface** *vlan-id*	-
Configure an IPX network number for the VLAN interface	**ipx network** *network*	Required By default, the system does not assign network numbers to VLAN interface. That is, IPX is disabled on all the VLAN interfaces
Enable IPX SAP	**undo ipx sap disable**	Required By default, SAP is enabled as soon as IPX is enabled on the VLAN interface

Configuring IPX SAP

In a large network, one IPX SAP broadcast consumes enormous bandwidth resources. By configuring an appropriate SAP update interval, you can reduce the bandwidth waste. Make sure that all servers and switches on the network have the same SAP update interval to avoid the situation where the switches mistake an operating server for a failed one.

The aging period of IPX SAP is a multiple of the IPX RIP update interval. You can set multiple update intervals as an aging period.

Table 89 Configure IPX SAP

Operation	Command	Description
Enter system view	**system-view**	-
Enable IPX	**ipx enable**	Required IPX is disabled by default
Configure the update interval of IPX SAP	**ipx sap timer update** *seconds*	Optional By default, the update interval of IPX SAP is 60 seconds

Table 89 Configure IPX SAP

Operation	Command	Description
Configure the aging period of IPX SAP	**ipx sap multiplier** *multiplier*	Optional By default, an IPX SAP service entry is deleted if it is not updated after three update intervals
Enter VLAN interface view	**interface Vlan-interface** *vlan-id*	-
Configure an IPX network number for the VLAN interface	**ipx network** *network*	Required By default, the system does not assign network numbers to VLAN interface. That is, IPX is disabled on all the VLAN interfaces
Enable IPX SAP	**undo ipx sap disable**	Required By default, SAP is enabled as soon as IPX is enabled on the VLAN interface
Configure the size of IPX SAP update packets	**ipx sap mtu** *bytes*	Optional By default, the maximum size of an IPX SAP update packet is 480 bytes. Each SAP update packet can carry up to seven sets of 64-byte service information

Configuring IPX GNS

Get nearest server (GNS) is a type of SAP message broadcasted by SAP-enabled NetWare clients. To the GNS requests, NetWare servers respond with GNS messages.

If a NetWare server is available on the network segment to which the client is connected, the server responds to its request. If no NetWare server is available on the segment, the switch responds.

You can enable the switch to handle a SAP GNS request in one of the following ways:

- Respond with the information of the nearest server (the server with the smallest hop count in the service information table on the switch).
- Respond with the information of one server that is picked out from all the known servers through round-robin polling.
- Respond depending on whether SAP GNS reply is enabled on the VLAN interface.

Table 90 Configure IPX GNS

Operation	Command	Description
Enter system view	**system-view**	-
Enable IPX	**ipx enable**	Required IPX is disabled by default

Table 90 Configure IPX GNS

Operation		Command	Description
Configure GNS reply of IPX SAP	Respond to GNS requests with the information of the server picked out by round-robin polling	**ipx sap gns-load-balance**	Optional By default, the switch responds to SAP GNS requests with the information of a server that is picked out in turn from all the known servers. This prevents a server from getting overloaded
	Respond to GNS requests with the information of the nearest server	**undo ipx sap gns-load-balance**	Optional By default, the switch responds to SAP GNS requests with the information of a server that is picked out in turn from all the known servers. This prevents a server from getting overloaded
Enter VLAN interface view		**interface Vlan-interface** *vlan-id*	-
Configure an IPX network number for the VLAN interface		**ipx network** *network*	Required By default, the system does not assign network numbers to VLAN interface. That is, IPX is disabled on all the VLAN interfaces
Disable GNS reply on the current VLAN interface		**ipx sap gns-disable-reply**	Optional By default, the VLAN interface responds to GNS requests

Configuring IPX service information

Generally, clients can only use the services that are advertised by NetWare servers and saved on the switch. To make a service always available to the clients, you can manually add it into the server information table as a static entry. If the route for the static service entry is invalid or deleted, the broadcast of the static service entry is disabled until the switch finds a valid route for the service entry.

IPX can support up to 10,240 service information entries with up to 5,120 service types and 5,120 static service information entries. You can configure the maximum service entries for one service type.

If the length of the new service information queue that you configure is less than the original one, the current service entries are not deleted. And if the number of the service entries of the same type reaches the specified value, new service information is not added.

Table 91 Configure IPX service information

Operation	Command	Description
Enter system view	**system-view**	-
Enable IPX	**ipx enable**	Required IPX is disabled by default

Table 91 Configure IPX service information

Operation	Command	Description
Configure a static IPX service entry	**ipx service** *service-type name network.node socket* **hop** *hops* [**preference** *preference*]	Optional By default, no static service entry is found in the service information table
Configure the maximum length of the service information reserve queue for one service type	**ipx sap max-reserve-servers** *length*	Optional By default, the maximum length of the service information reserve queue for one service type is 2,048

Configuring IPX forwarding

IPX RIP and SAP periodically broadcast update packets. If the periodical broadcast is not desired, you can enable triggered update on the VLAN interfaces of the switch. This allows the switch to broadcast update packets only when route or service information changes, thus avoiding broadcast flooding.

In some cases, split horizon must be disabled to ensure the correct transmission of routing information. Split horizon eliminates routing loops by forbidding the switch to send the routing information out of the interface where it is received. Disable split horizon only when necessary and with cautions, because it can result in routing loops.

Novell NetWare defines the type 20 IPX broadcast packet for the network basic input/output system (NetBIOS). You can enable/disable the forwarding of type 20 broadcast packets to other segments as required.

Table 92 Configure IPX forwarding

Operation	Command	Description
Enter system view	**system-view**	-
Enable IPX	**ipx enable**	Required IPX is disabled by default
Enter VLAN interface view	**interface Vlan-interface** *vlan-id*	-
Configure an IPX network number for the VLAN interface	**ipx network** *network*	Required By default, the system does not assign network numbers to VLAN interface. That is, IPX is disabled on all the VLAN interfaces
Enable triggered update of IPX	**ipx update-change-only**	Optional By default, triggered update of IPX is disabled
Enable split horizon of IPX	**ipx split-horizon**	Optional By default, split horizon is enabled
Configure the encapsulation format of the IPX frame	**ipx encapsulation** [**dot2** | **dot3** | **ethernet-2** | **snap**]	Optional By default, the encapsulation format of the IPX frame is 802.3 (**dot3**)

Table 92 Configure IPX forwarding

Operation	Command	Description
Enable the forwarding of type 20 broadcast packets	**ipx netbios-propagation**	Optional By default, type 20 broadcast packets are not forwarded

Displaying and Debugging IPX

After the above-mentioned configuration, use the **display** command in any view to view the running of IPX and to verify the effect of the configuration.

Use the **reset** command in user view to clear the IPX statistics.

Table 93 Display and debug IPX

Operation	Command	Description
Display the information of IPX on the VLAN interface	**display ipx interface** [**Vlan-interface** *vlan-id*]	The **display** command can be executed in any view
Display the IP packet statistics	**display ipx statistics**	
Display the IPX service information table	**display ipx service-table** [**inactive** | **name** *name* | **network** *network* | **order** { **network** | **type** } | **type** *service-type*] [**verbose**]	
Display the IPX routing information	**display ipx routing-table** [*network* [**verbose**] | **protocol** { **default** | **direct** | **rip** | **static** } [**inactive** | **verbose**] | **statistics** | **verbose**]	
Clear the IPX statistics	**reset ipx statistics**	The **reset** command can be executed in user view
Clear the IPX routing table information	**reset ipx routing-table statistics protocol** { **all** | **default** | **direct** | **rip** | **static** }	

IPX Configuration Example

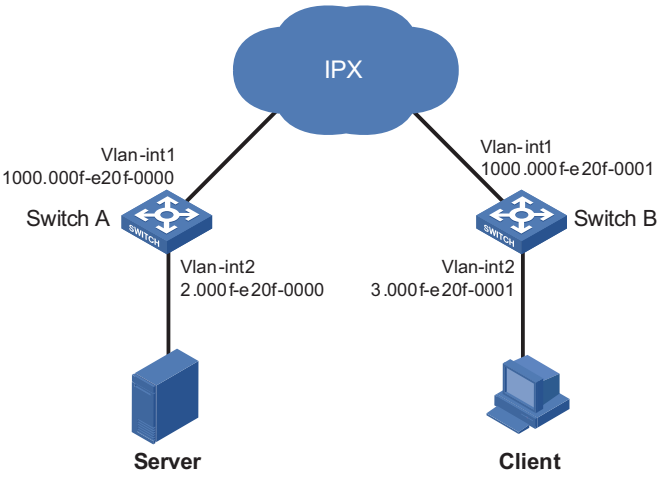
Network requirements

Through an IPX network, Switch A with the node address of 000f-e20f-0000 is connected to Switch B with the node address of 000f-e20f-0001.

There is a server installed with NetWare 4.1 and assigned the network number of 2. On the server, the packet encapsulation format is set to Ethernet_II. The client is a PC with the network number of 3 and the packet encapsulation format of SNAP. The server provides file service and printing service. The client accesses the file and printing services provided by the server through the IPX network. The node address of the server is 0000-0c91-f61f.

Network diagram

Figure 40 IPX network diagram



Configuration procedure

1 Configure Switch A.

Enable IPX.

```
<Switch> system-view
[Switch] ipx enable
```

Assign the network number 2 to VLAN interface 2 to enable IPX on the VLAN interface.

```
[Switch] interface Vlan-interface 2
[Switch-Vlan-interface2] ipx network 2
```

Set the packet encapsulation format to Ethernet_II on VLAN interface 2.

```
[Switch-Vlan-interface2] ipx encapsulation ethernet-2
[Switch-Vlan-interface2] quit
```

Assign the network number 1000 to VLAN interface 1 to enable IPX on the VLAN interface.

```
[Switch] interface Vlan-interface 1
[Switch-Vlan-interface1] ipx network 1000
```

Configure a static route with the destination network number 3.

```
[Switch-Vlan-interface1] quit
[Switch] ipx route-static 3 1000.000f-e20f-0001 tick 7 hop 2
```

2 Configure Switch B.

Enable IPX.

```
[Switch] ipx enable
```

Assign the network number 3 to VLAN interface 2 to enable IPX on the VLAN interface.

```
[Switch] interface Vlan-interface 2
[Switch-Vlan-interface2] ipx network 3
```

Set the packet encapsulation format to Ethernet_SNAP on VLAN interface 2.

```
[Switch-Vlan-interface2] ipx encapsulation snap
[Switch-Vlan-interface2] quit
```

Assign the network number 1000 to VLAN interface 1 to enable IPX on the VLAN interface.

```
[Switch] interface Vlan-interface 1
[Switch-Vlan-interface1] ipx network 1000
```

Configure a static route with the destination network number 2.

```
[Switch-Vlan-interface1] quit
[Switch] ipx route-static 2 1000.000f-e20f-0000 tick 7 hop 2
```

Configure a service information entry, indicating that Server can provide the file service.

```
[Switch] ipx service 4 fileserver 2.0000-0c91-f61f 451 hop 2
```

Configure a service information entry, indicating that the server can provide the printing service.

```
[Switch] ipx service 7 printserver 2.0000-0c91-f61f 5 hop 2
```

Troubleshooting IPX

Troubleshooting IPX forwarding

Symptom 1: A destination address cannot be pinged.

Solutions:

- Check whether the destination address is correct.
- Use the display ipx interface command to check whether the network number and IPX frame encapsulation format configured on the interface of the switch are consistent with those configured on the connected interface.
- Use the display ipx routing-table command to check whether the destination network is reachable.
- Use the debugging ipx packet command to enable debugging for IPX packets. Check whether IPX packets are correctly received, transmitted, forwarded, and dropped.

Symptom 2: Packets are dropped.

Solutions:

- If the IPX packet debugging information shows that a packet is dropped because "Packet size is greater than interface MTU!", perform the following

operations: Display the MTU setting on the VLAN interface with the display interface command and the RIP/SAP packet size with the display ipx interface command. Check whether the RIP/SAP packet size is smaller than the MTU setting on the VLAN interface.

Symptom 3: The switch cannot receive SAP packets.

Solutions:

- Use the display ipx interface command to check whether SAP is disabled on the VLAN interface.

Symptom 4: A type 20 IPX packet cannot be transmitted to other network segments.

Solutions:

- Use the display ipx interface command to check whether the forwarding of type 20 IPX packets is enabled on the input and output interfaces.
- Use the debugging ipx packet command to enable debugging for IPX packets. Check whether there is a prompt message of "Transport Control field of IPX type-20 packet >= 8!" A type 20 IPX packet can only be forwarded up to eight times; for the ninth forwarding attempt, the packet is dropped.

Troubleshooting IPX RIP

Symptom 1: The switch cannot learn routes from the peer device.

Solutions:

- Use the debugging ipx rip packet verbose command to enable debugging for IPX RIP. Check whether there is a RIP packet with routing information from the peer device to make sure that the underlying connection is available between the two devices.
- If there is a RIP packet with routing information from the peer device, you can use the debugging ipx rip event command to check whether the received routing information is added into the routing table.

Symptom 2: Try to import a static route to IPX RIP, but no static route is sent out.

Solutions:

- Use the display ipx routing-table command to check whether the static route exists.
- If the static route is not in the routing table, use the display ipx routing-table verbose command to check whether it exists as an inactive route. If the static route exists, check the inactive reason. When the route becomes active, it can be advertised as a RIP route.
- If the configured static route is shown in the routing table, check whether its hop count is smaller than 15.

Troubleshooting IPX SAP

Symptom 1: Unable to add static service information into the service information table.

Solutions:

- Use the display ipx service-table inactive command to check whether the service information is in the inactive service information table. If yes, there is no active route to the server.
- Check whether the number of service information entries exceeds the limitation with the display ipx service-table command. IPX can support 10,240 service information entries with up to 5,120 service types and 5,120 static service information entries.

Symptom 2: A service information entry cannot be found in the service information table.

Solutions:

- Use the display ipx service-table inactive command to check whether the service information is in the inactive service information table. If yes, there is no active route to the server.
- Check whether the VLAN interface is UP and SAP is enabled with the display ipx interface command.
- Check whether the hop count of the route to the server is smaller than 16 with the display ipx routing-table command.
- Check whether adequate memory is available for adding the service entry into the service information table. You can try to add it as a static service entry.

Symptom 3: No new dynamic service entry is found in the service information table.

Solutions:

- Check whether the relevant packets are received with the debugging ipx packet and debugging ipx sap packet verbose commands. If the packets are not received, the underlying network connection is unavailable.
- Use the ipx enable command to check whether IPX is enabled.
- Check whether IPX is configured on the VLAN interface with the display ipx interface command.
- Check whether SAP is enabled with the undo ipx sap disable command.
- Use the display ipx service-table command to check whether the number of SAP service entries is under the limit. IPX can support 10,240 service entries with 5,120 service types.
- Check whether the MTU of SAP packets is less than or equal to the MTU at the physical layer.

Symptom 4: No update packet is received on the VLAN interface.

Solutions:

- Check whether there are update packets with the debugging ipx packet and debugging ipx sap packet verbose commands. All the received/transmitted packets can be displayed through debugging information. If there are no update packets, check whether the underlying network connection is available.
- Use the display ipx interface command to check whether SAP is enabled.
- Check whether the hop count of the active route to the server is smaller than 16.
- Use the display current-configuration command to check whether the update interval is too long.
- Use the display current-configuration command to check whether the triggered updates feature is configured on the VLAN interface. Periodical update is disabled when the triggered updates feature applies.

Symptom 5: No update packets are sent out of the VLAN interface.

Solutions:

- Check whether there are update packets with the debugging ipx packet and debugging ipx sap packet verbose commands. Check whether the MTU of the SAP packets is smaller than the MTU of the VLAN interface to guarantee that they are not dropped by the underlying layer.
- Use the display current-configuration command to check whether the triggered updates feature is configured on the VLAN interface. Periodical update is disabled when the triggered updates feature applies.
- Check whether all service information is learnt from the VLAN interface. Then check whether split horizon is enabled on the VLAN interface.

Symptom 6: SAP does not respond to GNS requests.

Solutions:

- Use the debugging ipx packet sap command to check whether the switch receives the GNS packets.
- Check whether SAP is enabled on the VLAN interface.
- Use the display ipx interface command to check whether the VLAN interface is enabled to respond to GNS requests. If GNS reply is disabled, use the undo ipx sap gns-disable-reply command to enable the interface to respond to the GNS requests.
- Use the display ipx service table command to check whether the requested service information is available in the service information table.
- If the requested service information is available in the service information table, but SAP still does not give response, you need to check whether the service information is learnt from the interface where the request is received.

Symptom 7: SAP does not respond to a GNS request through Round-Robin.

Solutions:

- Use the display current-configuration command to check whether Round-Robin is enabled.

- If Round-Robin is enabled, check whether multiple equivalent service entries are available for the service request. The service entries are considered equivalent only when they have the same RIP delay, RIP hop count, SAP hop count and SAP preference.

Troubleshooting IPX routing management

Symptom 1: The current switch receives the routing information from a neighbor device, but the route cannot be found on the current switch with the **display ipx routing-table verbose** command.

Solutions:

- Use the display current-configuration command to view the maximum number of dynamic routes for each destination network number. The corresponding command is ipx route max-reserve-path. The default value is 4.
- Use the display ipx routing-table verbose command to check whether the number of the existing dynamic routes to the destination network is under the limit.
- If the number of dynamic route entries with the destination network number reaches the limit, use the ipx route max-reserve-path command to set a higher limit to accommodate new dynamic route information.

18 GVRP CONFIGURATION

Introduction to GARP and GVRP

Introduction to GARP

GARP (generic attribute registration protocol) offers a mechanism that is used by the members in the same switching network to distribute, propagate and register such information as VLAN and multicast addresses.

GARP dose not exist in a switch as an entity. A GARP participant is called GARP application. The main GARP applications at present are GVRP and GMRP. GVRP is described in the "GVRP Mechanism" on page 154 and GMRP will be described in Multicast Configuration. When a GARP participant is on a port of the switch, each port corresponds to a GARP participant.

Through GARP mechanism, the configuration information on one GARP member will be advertised rapidly in the whole switching network. GARP member can be a terminal workstation or bridge. A GARP member can notify other members to register or remove its attribute information by sending declarations or withdrawal declarations. It can also register or remove the attribute information of other GARP members according to the received declarations/withdrawal declarations.

GARP members exchange information through sending messages. There mainly are 3 types of GARP messages including Join, Leave, and LeaveAll.

- When a GARP participant wants to register its attribute information on other switches, it will send Join message outward.
- When it wants to remove some attribute values from other switches, it will send Leave message.
- LeaveAll timer will be started at the same time when each GARP participant is enabled and LeaveAll message will be sent upon timeout.

Leave message and LeaveAll message cooperate to ensure the logout and the re-registration of a message. Through exchanging messages, all the attribute information to be registered can be propagated to all the switches in the same switching network.

The destination MAC addresses of the packets of the GARP participants are specific multicast MAC addresses. A GARP-supporting switch will classify the packets received from the GARP participants and process them with corresponding GARP applications (GVRP or GMRP).

GARP and GMRP are described in details in the IEEE 802.1p standard (which has been added to the IEEE802.1D standard). 3Com Series Ethernet Switches fully support the GARP compliant with the IEEE standards.



- *The value of GARP timer will be used in all the GARP applications, including GVRP and GMRP, running in one switching network.*
- *In one switching network, the GARP timers on all the switching devices should be set to the same value. Otherwise, GARP application cannot work normally.*

GVRP Mechanism

GARP Timers

GARP timers include Hold timer, Join timer, Leave timer and LeaveAll timer.

- Hold: When a GARP participant receives a piece of registration information, it does not send out a Join message immediately. Instead, to save the bandwidth resources, it starts the Hold timer, puts all registration information it receives before the timer times out into one Join message and sends out the message after the timer times out.
- Join: To transmit the Join messages reliably to other entities, a GARP participant sends each Join message two times. The Join timer is used to define the interval between the two sending operations of each Join message.
- Leave: When a GARP participant expects to unregister a piece of attribute information, it sends out a Leave message. Any GARP participant receiving this message starts its Leave timer, and unregisters the attribute information if it does not receives a Join message again before the timer times out.
- LeaveAll: Once a GARP participant starts up, it starts the LeaveAll timer, and sends out a LeaveALL message after the timer times out, so that other GARP participants can re-register all the attribute information on this participant. After that, the participant restarts the LeaveAll timer to begin a new cycle.

GVRP port registration mode

GVRP has the following three port registration modes: Normal, Fixed, and Forbidden.

- Normal: In this mode, a port can dynamically register/deregister a VLAN and propagate the dynamic/static VLAN information.
- Fixed: In this mode, a port cannot register/deregister a VLAN dynamically. It only propagates static VLAN information. That is, a trunk port only permits the packets of manually configured VLANs in this mode even if you configure the port to permit the packets of all the VLANs.
- Forbidden: In this mode, a port cannot register/deregister VLANs. It only propagates VLAN 1 information. That is, a trunk port only permits the packets of the default VLAN (namely VLAN 1) in this mode even if you configure the port to permit the packets of all the VLANs.

GARP operation procedure

Through the mechanism of GARP, the configuration information on a GARP member will be propagated to the entire switched network. A GARP can be a terminal workstation or a bridge; it instructs other GARP member to register/unregister its attribute information by declaration/recant, and register/unregister other GARP member's attribute information according to other member's declaration/recant.

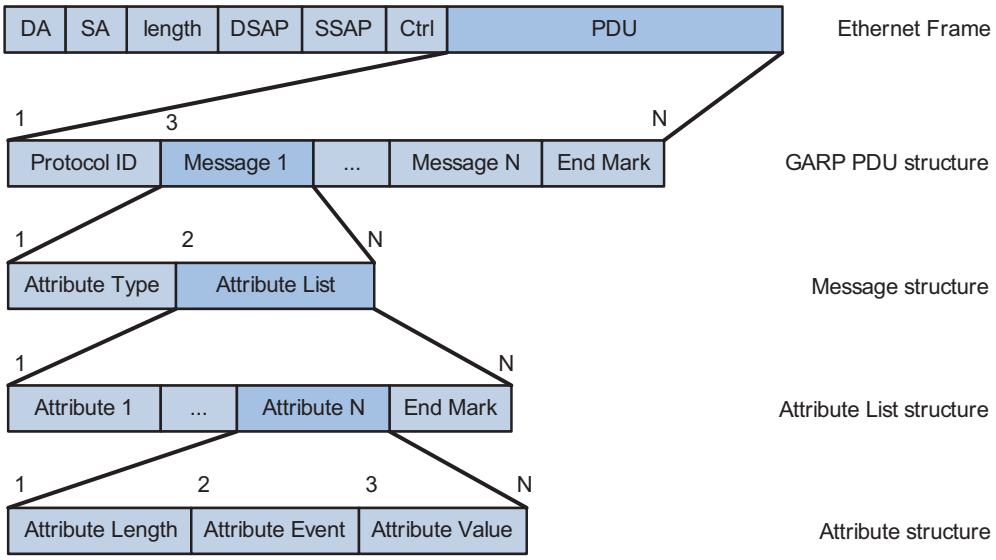
The protocol packets of GARP entity use specific multicast MAC addresses as their destination MAC addresses. When receiving these packets, the switch

distinguishes them by their destination MAC addresses and delivers them to different GARP application (for example, GVRP) for further processing.

GVRP Packet Format

The GVRP packets are in the following format:

Figure 41 Format of GVRP packets



The following table describes the fields of a GVRP packet.

Table 94 Description of GVRP packet fields

Field	Description	Value
Protocol ID	Protocol ID	1
Message	Each message consists of two parts: Attribute Type and Attribute List.	-
Attribute Type	Defined by the specific GARP application	The attribute type of GVRP is 0x01.
Attribute List	It contains multiple attributes.	-
Attribute	Each general attribute consists of three parts: Attribute Length, Attribute Event and Attribute Value. Each LeaveAll attribute consists of two parts: Attribute Length and LeaveAll Event.	-
Attribute Length	The length of the attribute	2 to 255
Attribute Event	The event described by the attribute	0: LeaveAll Event 1: JoinEmpty 2: JoinIn 3: LeaveEmpty 4: LeaveIn 5: Empty
Attribute Value	The value of the attribute	The attribute value of GVRP is the VID.

Table 94 Description of GVRP packet fields

Field	Description	Value
End Mark	End mark of the GVRP PDU.	The value of this field is fixed to 0x00.

Protocol Specifications

GVRP is defined in IEEE 802.1Q standard.

GVRP Configuration

The GVRP configuration tasks include configuring the GARP timers, enabling GVRP, and configuring the GVRP port registration mode.

Configuration Prerequisite

The port on which GVRP will be enabled must be set to a trunk port.

Configuration Procedure

Table 95 GVRP Configuration procedure

Operation	Command	Description
Enter system view	**system-view**	-
Configure the LeaveAll timer	**garp timer leaveall** *timer-value*	Optional By default, the LeaveAll timer is set to 1,000 centiseconds.
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Configure the Hold, Join, and Leave timers	**garp timer** { **hold** | **join** | **leave** } *timer-value*	Optional By default, the Hold, Join, and Leave timers are set to 10, 20, and 60 centiseconds respectively.
Exit and return to system view	**quit**	-
Enable GVRP globally	**gvrp**	Required By default, GVRP is disabled globally.
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Enable GVRP on the port	**gvrp**	Required By default, GVRP is disabled on the port. After you enable GVRP on a trunk port, you cannot change the port to a different type.
Configure GVRP port registration mode	**gvrp registration** { **fixed** | **forbidden** | **normal** }	Optional You can choose one of the three modes. By default, GVRP port registration mode is normal.

The timeout ranges of the timers vary depending on the timeout values you set for other timers. If you want to set the timeout time of a timer to a value out of the current range, you can set the timeout time of the associated timer to another value to change the timeout range of this timer.

The following table describes the relations between the timers:

Table 96 Relations between the timers

Timer	Lower threshold	Upper threshold
Hold	10 centiseconds	This upper threshold is less than or equal to one-half of the timeout time of the Join timer. You can change the threshold by changing the timeout time of the Join timer.
Join	This lower threshold is greater than or equal to twice the timeout time of the Hold timer. You can change the threshold by changing the timeout time of the Hold timer.	This upper threshold is less than one-half of the timeout time of the Leave timer. You can change the threshold by changing the timeout time of the Leave timer.
Leave	This lower threshold is greater than twice the timeout time of the Join timer. You can change the threshold by changing the timeout time of the Join timer.	This upper threshold is less than the timeout time of the LeaveAll timer. You can change the threshold by changing the timeout time of the LeaveAll timer.
LeaveAll	This lower threshold is greater than the timeout time of the Leave timer. You can change threshold by changing the timeout time of the Leave timer.	32,765 centiseconds



The recommended settings of GARP timers

- *GARP Hold timer: 100 centiseconds (1 second).*
- *GARP Join timer: 600 centiseconds (6 seconds).*
- *GARP Leave timer: 3000 centiseconds (30 seconds).*
- *GARP LeaveAll timer: 12000 centiseconds (2 minutes).*

Displaying and Maintaining GVRP

After the above configuration, you can use the **display** commands in any view to display the configuration information and operating status of GVRP/GARP, and thus verify your configuration. You can use the **reset** command in user view to clear GARP statistics.

Table 97 Display and maintain GVRP

Operation	Command	Description
Display GARP statistics	**display garp statistics** [**interface** *interface-list*]	The **display** commands can be executed in any view.
Display the settings of the GARP timers	**display garp timer** [**interface** *interface-list*]	
Display GVRP statistics	**display gvrp statistics** [**interface** *interface-list*]	
Display the global GVRP status	**display gvrp status**	
Clear GARP statistics	**reset garp statistics** [**interface** *interface-list*]	The **reset** command can be executed in user view.

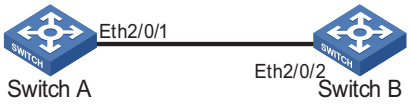
GVRP Configuration Example

Network requirements

You need to enable GVRP on the switches to enable dynamic VLAN information registration and update between the switches.

Network diagram

Figure 42 Network diagram for GVRP configuration



Configuration procedure

- Configure switch A.

Enable GVRP globally.

```
<SW7750> system-view
[SW7750] gvrp
GVRP is enabled globally.
```

Configure port Ethernet2/0/1 to be a trunk port and to permit the packets of all the VLANs.

```
[SW7750] interface Ethernet2/0/1
[SW7750-Ethernet2/0/1] port link-type trunk
[SW7750-Ethernet2/0/1] port trunk permit vlan all
```

Enable GVRP on the trunk port.

```
[SW7750-Ethernet2/0/1] gvrp
GVRP is enabled on port Ethernet2/0/1.
```

- Configure switch B.

Enable GVRP globally.

```
<SW7750> system-view
[SW7750] gvrp
GVRP is enabled globally.
```

Configure port Ethernet2/0/2 to be a trunk port and to permit the packets of all the VLANs.

```
[SW7750] interface Ethernet2/0/2
[SW7750-Ethernet2/0/2] port link-type trunk
[SW7750-Ethernet2/0/2] port trunk permit vlan all
```

Enable GVRP on the trunk port.

```
[SW7750-Ethernet2/0/2] gvrp
GVRP is enabled on port Ethernet2/0/2.
```

19 QinQ Configuration

QinQ Overview

Introduction to QinQ

The QinQ function enables packets to be transmitted across the operators' backbone networks with VLAN tags of private networks encapsulated in those of public networks. In public networks, packets of this type are transmitted by their outer VLAN tags (that is, the VLAN tags of public networks). And those of private networks which are encapsulated in the VLAN tags of public networks are shielded.

Figure 43 illustrates the structure of a packet with single VLAN tag.

Figure 43 Structure of the packets with single VLAN tag

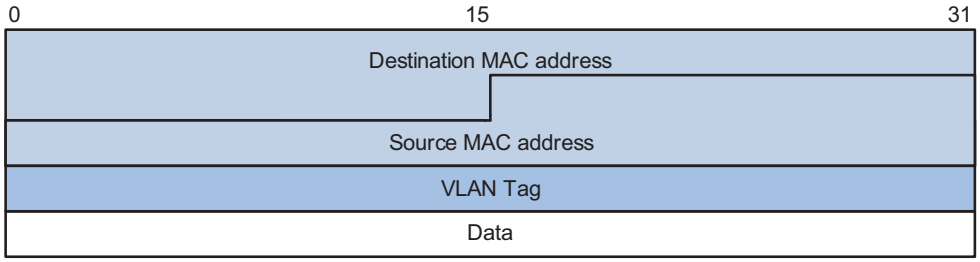
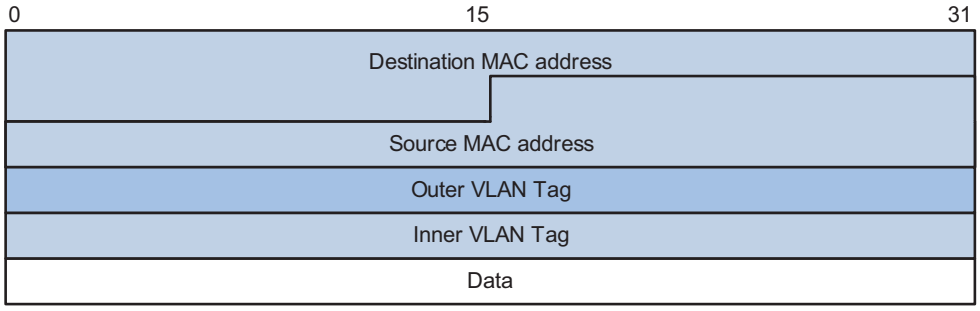


Figure 44 illustrates the structure of a packet with nested VLAN tags.

Figure 44 Structure of packets with nested VLAN tags



Compared with MPLS-based Layer 2 VPN, QinQ has the following features:

- It enables Layer 2 VPN tunnels that are simpler.
- QinQ can be implemented through manual configuration, without the support of signaling protocols.

The QinQ function provides you with the following benefits:

- Saves public network VLAN ID resource.
- You can have VLAN IDs of your own, which is independent of public network VLAN IDs.
- Provides simple Layer 2 VPN solutions for small-sized MANs or intranets.

Implementation of QinQ

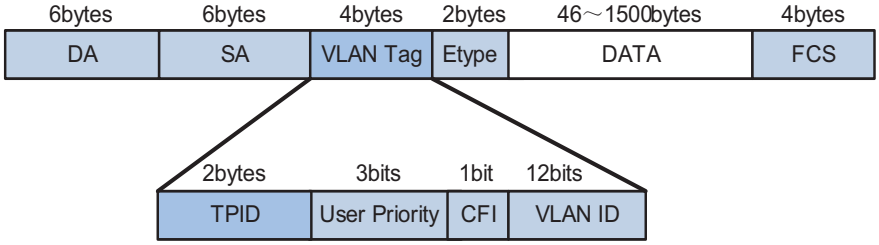
QinQ can be implemented by enabling the QinQ function on ports.

With the QinQ function enabled for a port, the switch will tag a received packet with the default VLAN tag of the receiving port no matter whether or not the packet already carries a VLAN tag, and the switch will learn the source MAC address of the packet into the MAC address table of the default VLAN. If the packet already carries a VLAN tag, the packet becomes a dual-tagged packet. Otherwise, the packet becomes a packet carrying the default VLAN tag of the port.

Inner-to-Outer Tag Priority Mapping

As shown in Figure 45, IEEE 802.1Q defines the structure of tagged packets in Ethernet frames:

Figure 45 The structure of tagged packets of Ethernet frames



The user priority field is the 802.1p priority of the tag. This 3-bit field is in the range of 0 to 7. Through configuring inner-to-outer tag priority mapping for a QinQ-enabled port, you can assign different priority for the outer tag of a packet according to its inner tag priority.

Refer to *"Setting Port Priority" on page 666* for the detailed configurations about priority mapping.

QinQ Configuration

Configuration Prerequisites

Make sure that Voice VLAN is not enabled for the port where QinQ is to be enabled. The QinQ feature is mutually exclusive with the Voice VLAN feature.

*BPDU tunnel is a specific application of the QinQ feature. The BPDU tunnel feature uses the **vlan-vpn tunnel** command to transmit the customers' MSTP packets transparently through the service provider's network. Refer to "BPDU Tunnel Configuration" on page 272.*

Configuration Procedure

Table 98 Configure QinQ

Operation	Command	Description
Enter system view	**system-view**	-

Table 98 Configure QinQ

Operation	Command	Description
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Enable QinQ for the port	**vlan-vpn enable**	Required By default, QinQ is disabled on a port.
Configure inner-to-outer tag priority mapping	**vlan-vpn priority** *inner-priority* **remark** *outer-priority*	Optional

The Voice VLAN feature is mutually exclusive with the QinQ feature for a port.

- When you use the specific command to enable the Voice VLAN feature for a QinQ-enabled port, the switch will prompt errors.
- If you use the **copy configuration** command to duplicate the configuration of a port to a QinQ-enabled port, the Voice VLAN feature is not duplicated.

CAUTION: *The 3C16863 and 3C16862 I/O Modules do not support the QinQ feature.*

Displaying QinQ

After the configuration above, you can verify QinQ configuration by executing the **display** command in any view.

Table 99 Display QinQ configuration

Operation	Command	Description
Display the QinQ configuration of all the ports	**display port vlan-vpn**	This command can be executed in any view.

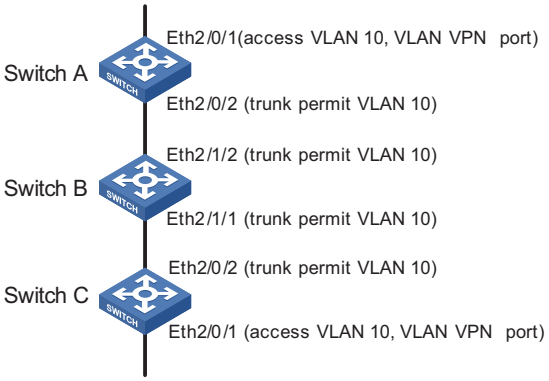
QinQ Configuration Example

Network requirements

- Switch A, Switch B, and Switch C are Switch 7750s.
- Two networks are connected to the Ethernet2/0/1 ports of Switch A and Switch C.
- Switch B only permits the packets of VLAN 10.
- It is required that packets of the VLANs other than VLAN 10 be exchanged between the networks connected to Switch A and Switch C.

Network diagram

Figure 46 Network diagram for QinQ configuration



Configuration procedure

1 Configure Switch A and Switch C.

As the configuration performed on Switch A and Switch C is the same, configuration on Switch C is omitted.

Configure Ethernet2/0/2 port as a trunk port. Add the port to VLAN 10.

```
<SwitchA> system-view
[SwitchA] vlan 10
[SwitchA-vlan10] quit
[SwitchA] interface Ethernet2/0/2
[SwitchA-Ethernet2/0/2] port link-type trunk
[SwitchA-Ethernet2/0/2] port trunk permit vlan 10
```

Enable QinQ for Ethernet2/0/1 port. Add the port to VLAN 10.

```
[SwitchA-Ethernet2/0/2] quit
[SwitchA] interface Ethernet2/0/1
[SwitchA-Ethernet2/0/1] port access vlan 10
[SwitchA-Ethernet2/0/1] stp disable
[SwitchA-Ethernet2/0/1] undo ntdp enable
[SwitchA-Ethernet2/0/1] vlan-vpn enable
[SwitchA-Ethernet2/0/1] quit
```

2 Configure Switch B.

Configure Ethernet2/0/1 port and Ethernet2/0/2 port as trunk ports. Add the two ports to VLAN 10.

```
<SwitchB> system-view
[SwitchB] vlan 10
[SwitchB-vlan10] quit
[SwitchB] interface Ethernet 2/0/1
[SwitchB-Ethernet2/0/1] port link-type trunk
[SwitchB-Ethernet2/0/1] port trunk permit vlan 10
[SwitchB-Ethernet2/0/1] quit
[SwitchB] interface Ethernet 2/0/2
[SwitchB-Ethernet2/0/2] port link-type trunk
[SwitchB-Ethernet2/0/2] port trunk permit vlan 10
```

The following describes how a packet is forwarded from Switch A to Switch C.

- *As QinQ is enabled on Ethernet2/0/1 port of Switch A, when a packet from the user's private network reaches Ethernet2/0/1 port of Switch A, it is tagged with the default VLAN tag of the port (VLAN 10 tag) and is then forwarded to Ethernet2/0/2 port.*
- *When the packet reaches Ethernet2/0/2 port of Switch B, it is forwarded in VLAN 10 and is passed to Ethernet2/0/1 port.*
- *The packet is forwarded from Ethernet2/0/1 port of Switch B to the network on the other side and reaches Ethernet2/0/2 port of Switch C. Switch C forwards the packet in VLAN 10 to its Ethernet2/0/1 port. As Ethernet2/0/1 port is an access port, the outer VLAN tag of the packet is stripped off and the packet restores the original one.*
- *It is the same case when a packet travels from Switch C to Switch A.*

After the configuration, the networks connecting Switch A and Switch C can receive packets from each other.

20 SELECTIVE QINQ CONFIGURATION

Selective QinQ Overview

Selective QinQ Implementation

On a Switch 7750 Ethernet switch, selective QinQ can be implemented in the following ways.

1 Enabling QinQ on ports

In this type of implementations, QinQ is enabled on ports and a received packet is tagged with the default VLAN tag of the receiving port no matter whether or not the packet already carries a VLAN tag. If the packet already carries a VLAN tag, the packet becomes a dual-tagged packet. Otherwise, the packet becomes a packet carrying the default VLAN tag of the port.

2 Configuring VLAN mapping

In this type of implementations, packets transmitted through the same port are tagged with outer VLAN tags according to the VLAN ID they carry. This is achieved by using the corresponding commands.



For Switch 7750 Ethernet switches, the selective QinQ feature can also be achieved through using ACL and QoS together. Refer to "Configuring Traffic-Based Selective QinQ" on page 679 for related configurations.

Outer Tag Replacement

Switch 7750s support the outer VLAN tag replacement function. You can specify one or more inner VLAN tags and an outer VLAN tag as a match rule. When receiving a double-tagged packet that matches the rule, the switch will replace the outer VLAN tag of the packet with a specified VLAN tag so that the packet will be forwarded as per the new outer VLAN tag, with the inner VLAN tag unchanged.

Selective QinQ Configuration

Configuring Selective QinQ

Configuration Prerequisites

- Enable QinQ in Ethernet port view.
- Set the VLANs whose packets are permitted the port.

Configuring Selective QinQ

Table 100 Configure selective QinQ

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Enable QinQ for the port	**vlan-vpn enable**	Required By default, QinQ is disabled.
Configure the outer VLAN tag to be added to a packet and configure the upstream port for this packet	**vlan-vpn vid** *vlan-id* **uplink** *interface-type interface-number* [**untagged**]	Required
Specify the inner VLAN tags by specifying VLAN IDs	**raw-vlan-id inbound** *vlan-id-list*	Required

CAUTION:

- *You need to execute the **vlan-vpn enable** command on the inbound ports before performing the operations listed in Table 100.*
- *QinQ is not applicable to ports with the Voice VLAN feature enabled.*

CAUTION:

- *Type-A I/O Modules do not support the selective QinQ feature. Type A I/O Modules include: 3C16860, 3C16861, LS81FS24A, 3C16858, 3C16859, and 32Gbps and 64Gbps Switch Fabrics.*
- *The 3C16863 and 3C16862 I/O Modules do not support the QinQ feature.*

Configuring Outer Tag Replacement

Table 101 Configure outer tag replacement

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Configure to replace the outer tag of matched packets with the specified tag of the specified VLAN, and enter QinQ view	**vlan-vpn vid** *vlan-id* **uplink** *interface-type interface-number* [**untagged**]	Required
Specify one or more inner VLAN tags and an outer VLAN tag as the match condition	**double-vlan-id inbound** *vlan-id-list* **outer-vid** *vlan-id*	Required By default, no match condition is defined

*The **double-vlan-id** command cannot be used while the **vlan-vpn enable** and **raw-vlan-id inbound** commands are in effect on the port.*

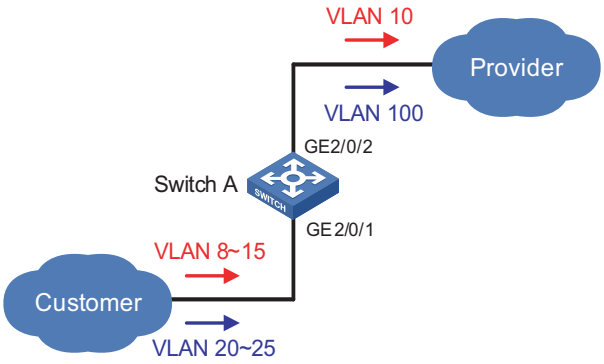
Selective QinQ Configuration Example

Network Requirements

- Switch A is a Switch 7750.
- Enable QinQ on GigabitEthernet2/0/1 port. Set the PVID of the port to 8.
- Insert the tag of VLAN 10 to packets of VLAN 8 through VLAN 15 as the outer VLAN tag. Insert the tag of VLAN 100 to packets of VLAN 20 through VLAN 25 as the outer VLAN tag.
- GigabitEthernet2/0/1 is the upstream port of the outer VLAN tag. It is required that the outer tags of packets of VLAN 10 and VLAN 100 are kept while the outer tags of packets of other VLANs are removed.

Network Diagram

Figure 47 Network diagram for selective QinQ configuration



Configuration Procedure

Enter system view.

```
<SwitchA> system-view
```

Enter GigabitEthernet2/0/1 port view.

```
[SwitchA] interface GigabitEthernet 2/0/1
```

Configure this port to be a hybrid port. And configure to keep the outer tags of packets of VLAN 10 and VLAN 100 and remove the outer tags of packets of other VLANs.

```
[SwitchA-GigabitEthernet2/0/1] port link-type hybrid
[SwitchA-GigabitEthernet2/0/1] port hybrid vlan 1 to 9 untagged
[SwitchA-GigabitEthernet2/0/1] port hybrid vlan 11 to 99 untagged
[SwitchA-GigabitEthernet2/0/1] port hybrid 101 to 4094 untagged
[SwitchA-GigabitEthernet2/0/1] port hybrid 10 tagged
[SwitchA-GigabitEthernet2/0/1] port hybrid 100 tagged
```

Enter GigabitEthernet2/0/1 port view.

```
[SwitchA] interface GigabitEthernet 2/0/1
```

Configure the port to be a hybrid port.

```
[SwitchA-GigabitEthernet2/0/1] port link-type hybrid
```

Configure the port to permit the packets of all the VLANs.

```
[SwitchA-GigabitEthernet2/0/1] port hybrid vlan 1 to 4094 untagged
```

Set the PVID of the port to 8.

```
[SwitchA-GigabitEthernet2/0/1] port hybrid pvid vlan 8
```

Enable QinQ.

```
[SwitchA-GigabitEthernet2/0/1] vlan-vpn enable
```

Specify the outer VLAN tag to be inserted to packets of VLAN 10, and specify the upstream port of the tag to be GigabitEthernet2/0/1 which does not remove the outer VLAN tags of packets when transmitting these packets.

```
[SwitchA-GigabitEthernet2/0/1] vlan-vpn vid 10 uplink GigabitEthernet 2/0/1
```

Specify the inner VLAN tags.

```
[SwitchA-GigabitEthernet2/0/1-vid-10] raw-vlan-id inbound 8 to 15
```

Specify the outer VLAN tag of VLAN 100 to be inserted to packets, and specify the upstream port of the tag to be GigabitEthernet2/0/1 which does not remove the outer VLAN tags of packets when transmitting these packets.

```
[SwitchA-GigabitEthernet2/0/1-vid-10] quit
[SwitchA-GigabitEthernet2/0/1] vlan-vpn vid 100 uplink GigabitEthernet 2/0/1
```

Specify the inner VLAN tags.

```
[SwitchA-GigabitEthernet2/0/1-vid-100] raw-vlan-id inbound 20 to 25
```

The above configuration causes the packets reaching GigabitEthernet2/0/1 port being processed as follows

- *Inserting VLAN 10 tag as the outer VLAN tag to single-tagged packets with their tags being that of VLAN 8 through VLAN 15.*
- *Inserting VLAN 100 tag as the outer VLAN tag to single-tagged packets with their tags being that of VLAN 20 through VLAN 25.*
- *Inserting VLAN 8 tag as the outer VLAN tag to single-tagged packets with their tags being neither that of VLAN 8 through VLAN 15 nor that of VLAN 20 through VLAN 25.*

21 SHARED VLAN CONFIGURATION

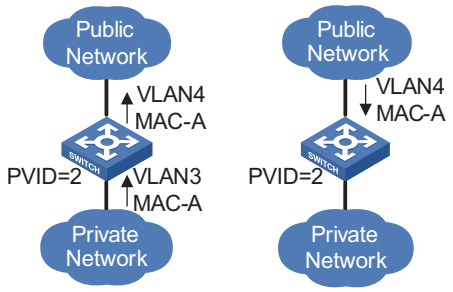
Shared VLAN Overview

Shared VLAN is special VLAN which is created based on I/O Modules of the device. It is designed to avoid packet broadcast in the applications of selective QinQ.

Generation of Shared VLAN

Like a QinQ-enabled port, a port with the selective QinQ enabled also learns the source MAC addresses of user packets to the MAC address table of the default VLAN of the port. However, the port with selective QinQ enabled can insert an outer VLAN tag besides the default VLAN tag to the packets. Thus, when packets from the service provider to customers are forwarded, broadcast arises because each of these packets fails to find its destination MAC address in the MAC table of its outer VLAN.

Figure 48 Learn MAC addresses of selective QinQ frames



As shown in Figure 48, when user packets are received, the default VLAN of the incoming port is VLAN 2, and the incoming port is specified to receive packets of VLAN 3, with outer tag of VLAN 4. When a packet is received, its source MAC address MAC-A is learned into the MAC address table of the default VLAN (VLAN 2) of the port.

When a response packet is returned to the device from VLAN 4 of the service provider network, the device will search the outgoing port for MAC-A in the MAC address table of VLAN 4. However, because the corresponding entry is not learned into the MAC address table of VLAN 4, this packet is considered to be a unicast packet with unknown destination MAC address. As a result, this packet will be broadcast to all the ports in VLAN 4, which wastes the network resources and endangers the network.

The problem above can be solved by using the shared VLAN feature, which summarizes the MAC address tables of all the VLANs. The switch can find the outgoing port for a packet according to the MAC address table of the shared VLAN and unicast the packet.

Working Principle of Shared VLAN

After shared VLAN is configured, all the MAC address entries learned by ports will be maintained on the MAC address forwarding table of the shared VLAN, which can be used to forward all the VLAN packets in the device.

With shared VLAN configured, the forwarding information about packets with the destination MAC address MAC-A learned by the customer port will be saved in the MAC address forwarding table of the shared VLAN. The packets received on the ports connected to the service provider can retrieve their forwarding path directly through looking up in the MAC address forwarding table of the shared VLAN. In this way, fewer unknown unicast packets will be broadcast by the device. As a result, the network resources are saved and the efficiency of the device is improved.

Shared VLAN Configuration

Configuring Shared VLAN on Fabric

Table 102 Configure shared VLAN on Fabric

Operation	Command	Description
Enter system view	**system-view**	-
Configure shared VLAN on Fabric	**shared-vlan** *vlan-id* **mainboard**	Required By default, no shared VLAN is configured on the Fabric.

For a Switch 7708R with two Fabrics equipped, the shared VLAN configured on the primary Fabric also takes effect on the secondary Fabric.

Configuring Shared VLAN on I/O Module

Table 103 Configure shared VLAN on I/O Module

Operation	Command	Description
Enter system view	**system-view**	-
Configure shared VLAN on I/O Module	**shared-vlan** *vlan-id* **slot** *slot-number*	Required By default, no shared VLAN is configured on the I/O Module.

With shared VLAN enabled, the packets of the current I/O Module or Fabric are forwarded according to the MAC address table of the shared VLAN. So you need to add the ports of all the packets to be forwarded to the shared VLAN. The operation of adding ports to the shared VLAN is the same as the operation of adding ports to a common VLAN. Refer to "Configuring a Port-Based VLAN" on page 97 for details.

CAUTION: *The shared VLAN can destroy RRPP rings and disable the RRPP feature, and thus cause rings in the network. So make sure that the RRPP feature and the shared VLAN feature is not enabled on a switch at the same time.*

Displaying Shared VLAN

After the above-mentioned configuration, you can execute the **display** command in any view to view the running information about the shared VLAN, so as to verify the configuration.

Table 104 Display shared VLAN

Operation	Command	Description
Display the shared VLANs configured for all the I/O Modules and Fabrics in the system	**display shared-vlan**	You can execute the **display** command in any view.

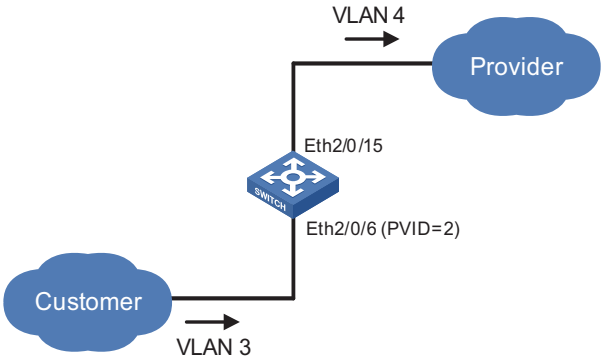
Shared VLAN Configuration Example

Network Requirements

- The selective QinQ feature is enabled on the hybrid port Ethernet2/0/6 which is connected to the customer network. The outer tag of VLAN 4 is inserted to packets of VLAN 3 in the customer network, and these tagged packets are transmitted to the service provider network through Ethernet2/0/15.
- Configure VLAN 100 as the shared VLAN on the module in slot 2 in order that any packet returned by the service provider can be unicast to the customer network.

Network Diagram

Figure 49 Network diagram for Shared VLAN configuration



Configuration Procedure

Enable selective QinQ on Ethernet2/0/6. Refer to "Selective QinQ Configuration Example" on page 167 for the details.

Specify VLAN 100 as the shared VLAN on the module in slot 2.

```
<SW7750> system-view
[SW7750] vlan 100
[SW7750-vlan100] quit
[SW7750] shared-vlan 100 slot 2
```

Add the ports of all the packets forwarded on the module in slot 2 to VLAN 100. Refer to *"Configuring a Port-Based VLAN" on page 97* for detailed configuration.

22 PORT BASIC CONFIGURATION

Ethernet Port Configuration

Configuring the Basic Settings of an Ethernet Port

Table 105 Configure the basic settings of an Ethernet port

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Enable the Ethernet port	**undo shutdown**	Optional By default, the port is enabled. Use the **shutdown** command to disable the port.
Set the description of the Ethernet port	**description** *text*	Optional By default, no description is defined for the port.
Set the duplex mode of the Ethernet port	**duplex** { **auto** | **full** | **half** }	Optional By default, the duplex mode of the port is **auto** (auto-negotiation).
Set the speed of the Ethernet port	**speed** { **10** | **100** | **1000** | **10000** | **auto** }	Optional By default, the speed of the port is **auto** (auto-negotiation).
Set the medium dependent interface (MDI) attribute of the Ethernet port	**mdi** { **across** | **auto** | **normal** }	Optional Be default, the MDI attribute of the port is **auto**.
Allow jumbo frames to pass through the Ethernet port	**jumboframe enable** [*jumboframe-value*]	Optional By default, jumbo frames that are larger than 1518 bytes and smaller than 1536 bytes are allowed to pass through the port.

Use the following two tables when setting the duplex mode and rate of an Ethernet port.

Table 106 Duplex mode setting for an Ethernet port

Port type	Duplex mode setting
100 Mbps electrical Ethernet port	It can work in full-duplex mode, half-duplex mode or auto-negotiation mode as required.
Gigabit electrical Ethernet port	It can work in full-duplex mode, half-duplex mode or auto-negotiation mode. However, if the rate is set to 1000 Mbps, its duplex mode can be set to **full** or **auto**.
100 Mbps optical Ethernet port	It works in full-duplex mode and its duplex mode can be set to **full** or **auto**.
Gigabit optical Ethernet port	It works in full-duplex mode and its duplex mode can be set to **full** or **auto**.
10,000 Mbps optical Ethernet port	Its duplex mode can be set to **full** only.
Management port	Its duplex mode cannot be set.

Table 107 Rate setting for an Ethernet port

Port type	Rate setting
100 Mbps electrical Ethernet port	Its rate can be set to 10 Mbps or 100 Mbps as required.
Gigabit electrical Ethernet port	Its rate can be set to 10 Mbps, 100 Mbps or 1000 Mbps as required. If its duplex mode is set to **full** or **half**, its rate cannot be set to 1000 Mbps.
100 Mbps optical Ethernet port	Its supports the rate of 100 Mbps. Its rate can be set to 100 Mbps or **auto**.
Gigabit optical Ethernet port	Its supports the rate of 1000 Mbps. Its rate can be set to 1000 Mbps or **auto**.
10,000 Mbps optical Ethernet port	Its rate can be set to 10,000 Mbps only.
Management port	Its rate cannot be set.

Configuring Port Auto-Negotiation Speed

You can configure an auto-negotiation speed for a port by using the **speed auto** command.

Take a 10/100/1000 Mbps port as an example.

- If you expect that 10 Mbps is the only available auto-negotiation speed of the port, you just need to configure **speed auto 10**.
- If you expect that 10 Mbps and 100 Mbps are the available auto-negotiation speeds of the port, you just need to configure **speed auto 10 100**.
- If you expect that 10 Mbps and 1000 Mbps are the available auto-negotiation speeds of the port, you just need to configure **speed auto 10 1000**.

Table 108 Configure auto-negotiation speeds for a port

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter Ethernet interface view	**interface** *interface-type interface-number*	-

Table 108 Configure auto-negotiation speeds for a port

Operation	Command	Remarks
Configure the available auto-negotiation speed(s) for the port	**speed auto** [**10** | **100** | **1000**]*	Optional ■ By default, the port speed is determined through auto-negotiation. ■ Use the **1000** keyword for Gigabit Ethernet ports only

- *Only ports on the front panel of the device support the auto-negotiation speed configuration feature. And ports on the extended interface module do not support this feature currently.*
- *After you configure auto-negotiation speed(s) for a port, if you execute the **undo speed** command or the **speed auto** command, the auto-negotiation speed setting of the port restores to the default setting.*
- *The effect of executing **speed auto 10 100 1000** equals to that of executing **speed auto**, that is, the port is configured to support all the auto-negotiation speeds: 10 Mbps, 100 Mbps, and 1000 Mbps.*

Configuring Broadcast/Multicast/Unknown Unicast Suppression

By performing the following configurations, you can limit different types of incoming traffic on individual ports. When a type of incoming traffic exceeds the threshold you set, the system drops the packets exceeding the traffic limit to reduce the traffic ratio of this type to the reasonable range, so as to keep normal network service.

Table 109 Configure broadcast/multicast/unknown unicast suppression

Operation	Command	Description
Enter system view	**system-view**	-
Suppress broadcast traffic received on all ports in the current VLAN	**broadcast-suppression** { *ratio* | **pps** *pps* }	Optional By default, the switch does not suppress broadcast traffic
Exit VLAN view	**quit**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Limit broadcast traffic received on the current port	**broadcast-suppression** { *ratio* | **bandwidth** *bandwidth* | **pps** *pps* }	Optional By default, the switch does not suppress broadcast traffic.
Limit multicast traffic received on the current port	**multicast-suppression** { *ratio* | **bandwidth** { *mbps-value* | **kbps** *kbps-value* } | **pps** *max-pps* }	Optional By default, the switch does not suppress multicast traffic.
Limit unknown unicast traffic received on the current port	**unicast-suppression** { *ratio* | **bandwidth** { *mbps-value* | **kbps** *kbps-value* } | **pps** *max-pps* }	Optional By default, the switch does not suppress unknown unicast traffic.

Type-A I/O Modules, including 3C16860, 3C16861, LS81FS24A, 3C16858, and 3C16859, do not support enabling broadcast/multicast/unknown unicast suppression on ports.

Enabling Flow Control on a Port

Flow control is enabled on both the local and peer switches. If congestion occurs on the local switch:

- The local switch sends a message to notify the peer switch of stopping sending packets to itself temporarily.
- The peer switch will stop sending packets to the local switch or reduce the sending rate temporarily when it receives the message; and vice versa. By this way, packet loss is avoided and the network service operates normally.

Table 110 Enable flow control on a port

Operation	Command	Description
Enter system view	**system-view**	-
Enable flow control globally	**flow-control enable**	Required By default, flow control is disabled globally.
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Enable flow control on the Ethernet port	**flow-control**	Required By default, flow control is disabled on the port.

Configuring a Delay for Reporting a Port Physically Down Event

The physical state of an Ethernet port is either up or down. In normal cases, immediately after the physical state changes, the port reports the event to the system. This can be resource consuming when state changing is frequent in a short period of time.

You can address the problem by introducing a delay for reporting the physically down event of a port. With this delay, a port reports a physically down event after the delay expires rather than doing that immediately upon occurrence of the down event. You can thus affect how soon the system can obtain the physical state of its ports.

Table 111 Configure a delay for reporting a port physically down event

Operation	Command	Description
Enter system view	**system-view**	-
Set the delay of reporting down state for the ports of all I/O Modules or the specified I/O Module	**port monitor last** [**slot** *slot-number*] *value*	Optional By default, the report delay is 1.
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Set the down event reporting delay on the current port	**port monitor last** [*value*]	Optional By default, the delay setting is the same as the global setting in system view.



- *The delays set with the above commands are weight values rather than exact time values. The greater the delay weight, the longer the delay.*
- *You can set the delay of reporting down state either in system view or Ethernet port view. If you perform this configuration in both system view and Ethernet port view, the configuration performed in Ethernet port view is given priority.*

Copying the Configuration of a Port to Other Ports

To make some other ports have the same configuration as that of a specific port, you can copy the configuration of the specific port to the ports.

Specifically, the following types of port configuration can be copied from one port to other ports: VLAN configuration, protocol-based VLAN configuration, LACP configuration, QoS configuration, STP configuration and initial port configuration. The other configurations cannot be copied temporarily.

- VLAN configuration: includes IDs of the VLANs allowed on the port and the default VLAN ID of the port;
- Protocol-based VLAN configuration: includes IDs and indexes of the protocol-based VLANs allowed on the port;
- Link aggregation control protocol (LACP) configuration: includes LACP enable/disable status;
- QoS configuration: includes rate limit, port priority, and default 802.1p priority on the port;
- STP configuration: includes STP enable/disable status on the port, link attribute on the port (point-to-point or non-point-to-point), STP priority, path cost, packet transmission rate limit, whether loop protection is enabled, whether root protection is enabled, and whether the port is an edge port;
- Port configuration: includes link type of the port, port rate and duplex mode.

Table 112 Copy the configuration of a port to other ports

Operation	Command	Description
Enter system view	**system-view**	-
Copy the configuration of a port to other ports	**copy configuration source** { *interface-type interface-number* | **aggregation-group** *source-agg-id* } **destination** { *interface-list* [**aggregation-group** *destination-agg-id*] | **aggregation-group** *destination-agg-id* }	Required



- *To copy the configuration of a source port to a member port of a link aggregation group, you should configure the aggregation group rather than the member port itself as the destination port. If the member port is configured as the destination port, the switch will remove the port from the destination port list, resulting configuration copy failure for the port.*
- *If you specify a source aggregation group ID, the system will use the port with the smallest port number in the aggregation group as the source.*
- *If you specify a destination aggregation group ID, the configuration of the source port will be copied to all ports in the aggregation group and all ports in the group will have the same configuration as that of the source port.*
- *The **copy** command cannot copy the configuration of a port to a reflector port.*
- *The **copy** command cannot copy the configuration of a port to the destination port of a mirroring group.*

Configuring Loopback Detection for a Port

Loopback detection is used to monitor if loopback occurs on a switch port.

After you enable loopback detection on Ethernet ports, the switch can monitor if external loopback occurs on each port periodically. If loopback occurs on a port, the system will process the port in the user-defined mode.

Table 113 Set loopback detection for a port

Operation	Command	Description
Enter system view	**system-view**	-
Set time interval for port loopback detection	**loopback-detection interval-time** *time*	Optional The default interval is 30 seconds.
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Enable loopback detection on the specified port	**loopback-detection enable**	Required By default, loopback detection is disabled by default.
Set the processing mode for the port where loopback is detected	**loopback-detection control** { **block** | **nolearning** | **shutdown** }	Optional By default, the port where loopback is detected is blocked.
Configure the system to detect loopback in all the VLANs where the current Trunk port or Hybrid port resides	**loopback-detection per-vlan enable**	Optional By default, the system detects loopback only in the default VLAN of the current Trunk port or hybrid port.

Enabling the System to Test Connected Cable

You can enable the system to test the cable connected to a specific port. The test result will be returned in five minutes. The system can test these attributes of the cable: Receive and transmit directions (RX and TX), short circuit/open circuit or not, the length of the faulty cable.

Table 114 Enable the system to test connected cables

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Enable the system to test connected cables	**virtual-cable-test**	Required

Configuring the Interval to Perform Statistical Analysis on Port Traffic

By performing the following configuration, you can set the interval to perform statistical analysis on the traffic of a port.

When you use the **display interface** *interface-type interface-number* command to display the information of a port, the system performs statistical analysis on the traffic flow passing through the port during the specified interval and displays the average rates in the interval. For example, if you set this interval to 100 seconds, the displayed information is as follows:

```
Last 100 seconds input:  0 packets/sec 0 bytes/sec
 Last 100 seconds output:  0 packets/sec 0 bytes/sec
```

Table 115 Set the interval to perform statistical analysis on port traffic

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Set the interval to perform statistical analysis on port traffic	**flow-interval** *interval*	Optional By default, this interval is 300 seconds.

Setting Speedup for a Port

Perform the following configuration to speed up the hardware in a port or out of a port.

Table 116 Set speedup for a port

Operation	Command	Description
Enter system view	**system-view**	-
Enable the hardware speedup function inside the port	**hardspeedup enable**	Optional By default, the hardware speedup function inside the port is enabled.
Disable the hardware speedup function inside the port	**hardspeedup disable**	
Enable the hardware speedup function outside the port	**speedup enable**	Optional By default, the hardware speedup function outside the port is enabled.
Disable the hardware speedup function outside the port	**speedup disable**	

CAUTION:

- *The hardspeedup enable/disable commands are applicable to type-A I/O Modules only, including 3C16860, 3C16861, LS81FS24A, 3C16858, and 3C16859.*
- *The speedup enable/disable commands are applicable to non-type-A I/O Modules only.*
- *The commands above are diagnostic, so you cannot use them at discretion.*

Controlling UP/Down Log Output on a Port

An Ethernet port has two physical link statuses: UP and Down. When the state of an Ethernet port changes, the switch will send log information to the log server, which then responds accordingly. If the status of Ethernet ports changes frequently, the switch will send log information to the log server frequently, burdening the log server and consuming plenty of network resources.

To solve the problem, you can use the Up/Down log information output control function. By using the function, you can choose to monitor certain Ethernet ports instead of monitoring all ports, so as to reduce the quantity of log information output to the log server.

After you allow a port to output the Up/Down log information, if the physical link status of the port does not change, the switch does not send log information to the log server but monitors the port in real time.

Table 117 Allow a port to output the UP/Down log information

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Allow the port to output the UP/Down log information	**enable log updown**	Required By default, a port is allowed to output the UP/Down log information.

Displaying Basic Port Configuration

After the above configurations, you can execute the **display** commands in any view to display information about Ethernet ports, so as to verify your configurations.

You can execute the **reset counters interface** command in user view to clear the statistics of Ethernet ports.

Table 118 Display basic port configuration

Operation	Command	Description
Display port configuration information	**display interface** [*interface-type* | *interface-type interface-number*]	You can execute the **display** commands in any view.
Display the information about port loopback detection	**display loopback-detection** [**port-loopbacked**] [**|** { **begin** | **include** | **exclude** } *regular-expression*]	
Display brief information about port configuration	**display brief interface** [*interface-type interface-number*] [**|** { **begin** | **include** | **exclude** } *string*]	
Display port information about a specified unit	**display unit** *unit-id* **interface**	
Clear port statistics	**reset counters interface** [*interface-type* | *interface-type interface-number*]	You can execute the **reset** command in user view. After 802.1x is enabled on a port, clearing the statistics on the port will not work.

Ethernet Port Configuration Example

Network requirements

- Switch A and Switch B are connected to each other through two trunk port (Ethernet2/0/1).
- Configure the default VLAN ID of both Ethernet2/0/1 to 100.
- Allow the packets of VLAN 2, VLAN 6 through VLAN 50 and VLAN 100 to pass both Ethernet2/0/1.

Network diagram

Figure 50 Network diagram for Ethernet port configuration



Configuration procedure

- *Only the configuration for Switch A is listed below. The configuration for Switch B is similar to that of Switch A.*
- *This example supposes that VLAN 2, VLAN 6 through VLAN 50 and VLAN 100 have been created.*

Enter Ethernet port view of Ethernet2/0/1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface ethernet2/0/1
```

Set Ethernet2/0/1 as a trunk port.

```
[SW7750-Ethernet2/0/1] port link-type trunk
```

Allow packets of VLAN 2, VLAN 6 through VLAN 50 and VLAN 100 to pass Ethernet2/0/1.

```
[SW7750-Ethernet2/0/1] port trunk permit vlan 2 6 to 50 100
```

Configure the default VLAN ID of Ethernet2/0/1 to 100.

```
[SW7750-Ethernet2/0/1] port trunk pvid vlan 100
```

Troubleshooting Ethernet Port Configuration

Symptom: Fail to configure the default VLAN ID of a port.

Solution: Take the following steps.

- Use the **display interface** or **display port** command to check if the port is a trunk port or a hybrid port. If not, configure it to a trunk port or a hybrid port.
- Configure the default VLAN ID.

23 LINK AGGREGATION CONFIGURATION

Overview

Introduction to Link Aggregation

Link aggregation aggregates multiple physical Ethernet ports into one logical link, also called an aggregation group. It allows you to increase bandwidth by distributing incoming/outgoing traffic on the member ports in the aggregation group. In addition, it provides reliable connectivity because these member ports can dynamically back up each other.

Depending on different aggregation modes, aggregation groups fall into three types: manual, static LACP, and dynamic LACP. Depending on whether or not load sharing is implemented, aggregation groups can be load-sharing or non-load-sharing aggregation groups.

For the member ports in an aggregation group, their basic configuration must be the same. The basic configuration includes STP, QoS, VLAN, port attributes and other associated settings.

- STP configuration, including STP status (enabled or disabled), link attribute (point-to-point or not), STP priority, maximum transmission speed, loop prevention status, root protection status, edge port or not.
- QoS configuration, including traffic limiting, priority marking, default 802.1p priority, bandwidth assurance, congestion avoidance, traffic redirection, traffic statistics, and so on.
- VLAN configuration, including permitted VLANs, and default VLAN ID.
- Port attribute configuration, including port rate, duplex mode, and link type (Trunk, Hybrid or Access). The ports for a manual or static aggregation group must have the same link type, and the ports for a dynamic aggregation group must have the same rate, duplex mode and link type.

Introduction to LACP

The purpose of the link aggregation control protocol (LACP) is to implement dynamic link aggregation and deaggregation. This protocol is defined in IEEE802.3ad. It uses link aggregation control protocol data units (LACPDUs) for information exchange between LACP-enabled devices.

After LACP is enabled on a port, the port sends LACPDUs to notify the remote system of its system LACP priority, system MAC address, port LACP priority, port number, and operational key. Upon receipt of an LACPDU, the remote system compares the received information with the information received on other ports to determine the ports that can operate as selected ports. This allows the two systems to reach an agreement on the states of the related ports.

Operational Key

When aggregating ports, link aggregation control automatically assigns each port an operational key based on its rate, duplex mode, and other basic configurations.

- In a manual or static LACP aggregation group, the selected ports share the same operational key.
- In a dynamic LACP aggregation group, all ports share the same operational key

Manual Aggregation Group

Introduction to manual aggregation group

A manual aggregation group is manually created. All its member ports are manually added and can be manually removed (it inhibits the system from automatically adding/removing ports to/from it). Each manual aggregation group must contain at least one port. When a manual aggregation group contains only one port, you cannot remove the port unless you remove the whole aggregation group.

LACP is disabled on the member ports of manual aggregation groups, and enabling LACP on such a port will not take effect.

Port status in manual aggregation group

A port in a manual aggregation group can be in one of the two states: selected or standby. The selected port with the minimum port number serves as the master port of the group, and other selected ports serve as member ports of the group.

There is a limit on the number of selected ports in an aggregation group. Therefore, if the number of the member ports that can be set as selected ports in an aggregation group exceeds the maximum number supported by the device, the system will choose the ports with lower port numbers as the selected ports, and set others as standby ports.

Requirements on ports for manual aggregation

Generally, there is no limit on the rate and duplex mode of the ports you want to add to a manual aggregation group. However, the following cases will be processed differently:

- For the ports which are initially down, there is no limit on the rate and duplex mode of the ports when they are added to an aggregation group;
- For the currently down ports which used to be up and whose rate and duplex mode are specified in the negotiation mode or mandatory mode, the rate and duplex mode of each port must be the same as those of other ports when they are aggregated;
- When the rate and duplex mode of a port in the manual aggregation group change, the system does not deaggregate the aggregation group and all the ports in the group work normally. However, if the rate of the master port decreases and the duplex mode of the master port changes, the packets forwarded on the port may be dropped.

Static LACP Aggregation Group

Introduction to static LACP aggregation

A static LACP aggregation group is also manually created. All its member ports are manually added and can be manually removed (it inhibits the system from automatically adding/removing ports to/from it). Each static aggregation group must contain at least one port. When a static aggregation group contains only one

port, you cannot remove the port unless you remove the whole aggregation group.

LACP is enabled on the member ports of static aggregation groups, and disabling LACP on such a port will not take effect. When you remove a static aggregation group, the system will remain the member ports of the group in LACP-enabled state and re-aggregate the ports to form one or more dynamic LACP aggregation groups.

Port status of static aggregation group

A port in a static aggregation group can be in one of the two states: selected or standby. Both the selected and the standby ports can transceive LACPDUs however, the standby ports cannot forward user packets.

In an aggregation group, the selected port with the minimum port number serves as the master port of the group, and other selected ports serve as member ports of the group.

In a static aggregation group, the system sets the ports to selected or standby state according to the following rules:

- The system sets the "most preferred" ports (that is, the ports take most precedence over other ports) to selected state, and others to standby state. Port precedence descends in the following order: full duplex/high speed, full duplex/low speed, half duplex/high speed, half duplex/low speed.
- The system sets the following ports to standby state: ports that are not connected to the same peer device as the master port (selected port with the minimum port number), and ports that are connected to the same peer device as the master port but not in the same aggregation group as the master port.
- The system sets the ports unable to aggregate with the master port (due to some hardware limit, for example, cross-board aggregation unavailability) to standby state.
- The system sets the ports with basic port configuration different from that of the master port to standby state.

There is a limit on the number of selected ports in an aggregation group. Therefore, if the number of the member ports that can be set as selected ports in an aggregation group exceeds the maximum number supported by the device, the system will choose the ports with lower port numbers as the selected ports, and set others as standby ports.

For the restriction of I/O Module types on link aggregation, refer to Table 120 and Table 121.

Dynamic LACP Aggregation Group

Introduction to dynamic LACP aggregation group

A dynamic LACP aggregation group is automatically created and removed by the system. Users cannot add/remove ports to/from it. Ports can be aggregated into a dynamic aggregation group only when they are connected to the same peer device and have the same basic configuration (such as rate and duplex mode).

Besides multiple-port aggregation groups, the system is also able to create single-port aggregation groups, each of which contains only one port. LACP is enabled on the member ports of dynamic aggregation groups.

Port status of dynamic aggregation group

A port in a dynamic aggregation group can be in one of the two states: selected or standby. In a dynamic aggregation group, both the selected and the standby ports can transceive LACPDUs, however, the standby ports cannot forward user packets.

There is a limit on the number of selected ports in an aggregation group. Therefore, if the number of the member ports that can be set as selected ports in an aggregation group exceeds the maximum number supported by the device, the system will negotiate with its peer end, to determine the states of the member ports according to the port IDs of the preferred device (that is, the device with smaller system ID). The following is the negotiation procedure:

1. Compare device IDs (system priority + system MAC address) between the two parties. First compare the two system priorities, then the two system MAC addresses if the system priorities are equal. The device with smaller device ID will be considered as the preferred one.
2. Compare port IDs (port priority + port number) on the preferred device. The comparison between two port IDs is as follows: First compare the two port priorities, then the two port numbers if the two port priorities are equal; the port with the smallest port ID is the selected port and the left ports are standby ports.

   In an aggregation group, the selected port with the minimum port number serves as the master port of the group, and other selected ports serve as member ports of the group.



- *The down ports in a static aggregation group or dynamic aggregation group are standby ports, which is different in manual aggregation groups.*
- *For the restriction of I/O Module types on link aggregation, refer to Table 120 and Table 121.*

Restriction of I/O Module Types on Link Aggregation

Table 119 lists link aggregation types and related descriptions.



Type-A modules (I/O Module) include 3C16860, 3C16860, 3C16861, 3C16861, LS81FS24A, LS81FS24, 3C16858, 3C16858, 3C16859, and 3C16859.

Table 119 Link aggregation types and related descriptions

Aggregation type	Basic description	Specific description
Manual aggregation	Support up to 384 aggregation groups, including 64 load sharing aggregation groups	■ For Type-A modules, an aggregation group supports up to 8 selected GE ports or 16 selected FE ports ■ For non-Type-A modules, an aggregation group supports up to 8 selected GE ports or 8 selected FE ports
Static/dynamic aggregation		■ For Type-A modules, an aggregation group supports up to 8 selected GE ports ■ For Type-A modules, an aggregation group supports up to 24 FE ports, including up to 16 selected ones ■ For non-Type-A modules, an aggregation group supports up to 48 ports, including up to 8 selected ones

If devices at one side of the link aggregation group use type-A modules and devices at the other side of the group use modules other than Type A, when the number of ports exceeds eight and the number of selected ports reaches to eight in the link aggregation group, packets may be lost.

Table 120 and Table 121 describe the restriction of type-A I/O Modules and non-type-A I/O Modules on link aggregation respectively.

Table 120 Restriction of type-A I/O Modules on link aggregation

I/O Module type	Cross-chip aggregation	Aggregation type	I/O Module specification	Maximum number of ports in an aggregation group	Maximum number of selected ports in an aggregation group
Type-A I/O Module	Not supported	Manual aggregation	3C16860/3C16860	16	16
			3C16861/LS81FS24A/3C16861/LS81FS24	16	16
			3C16858/3C16859/3C16858/3C16859	8	8
		Static/dynamic aggregation	3C16860/3C16860	24	16
			3C16861/LS81FS24A/3C16861/LS81FS24	24	16
			3C16858/3C16859/3C16858/3C16859	8	8

Table 121 Restriction of non-type-A I/O Modules on link aggregation

I/O Module type	Cross-chip aggregation	Aggregation type	Maximum number of ports in an aggregation group	Maximum number of selected ports in an aggregation group
Non-type-A I/O Module	Supported	Manual aggregation	8	8
		Static/dynamic aggregation	The number of ports on the I/O Module	8

Aggregation Group Categories

Depending on whether or not load sharing is implemented, aggregation groups can be load-sharing or non-load-sharing aggregation groups.

In general, the system only provides limited load-sharing aggregation resources, so the system needs to reasonably allocate the resources among different aggregation groups.

The system always allocates hardware aggregation resources to the aggregation groups with higher priorities. When load-sharing aggregation resources are used up by existing aggregation groups, newly-created aggregation groups will be non-load-sharing ones.

The priorities of aggregation groups for allocating load-sharing aggregation resources are as follows:

- An aggregation group containing special ports (such as 10GE port) which require hardware aggregation resources has higher priority than any aggregation group containing no special port.
- A manual or static aggregation group has higher priority than a dynamic aggregation group (unless the latter contains special ports while the former does not).
- For two aggregation groups of the same kind, the one that might gain higher speed if resources were allocated to it has higher priority than the other one.
- If the two groups can gain the same speed after resources are allocated to them, the one with smaller master port number has higher priority than the other one.

When an aggregation group of higher priority appears, the aggregation groups of lower priorities release their hardware resources. For single-port aggregation groups, if they can transceive packets normally without occupying aggregation resources, they will not occupy hardware aggregation resources.



CAUTION: *A load-sharing aggregation group contains up to two selected ports, however, a non-load-sharing aggregation group can only have one selected port at most and others are standby ports.*

Link Aggregation Configuration



CAUTION:

- *The following ports cannot be added to an aggregation group: destination ports to be mirrored to, reflection ports to be remotely mirrored to, ports configured with static MAC addresses, static-ARP-enabled ports, and 802.1x-enabled ports.*
- *Ports with IP-MAC address binding configured cannot be added to an aggregation group.*
- *A port with port security enabled cannot be added to an aggregation group.*

Configuring a Manual Aggregation Group

You can create a manual aggregation group, or remove an existing manual aggregation group (after that, all the member ports in the group are removed from the ports).

You can manually add/remove a port to/from a manual aggregation group, and a port can only be manually added/removed to/from a manual aggregation group.

Table 122 Configure a manual aggregation group

Operation	Command	Description
Enter system view	**system-view**	-
Create a manual aggregation group	**link-aggregation group** *agg-id* **mode manual**	Required

Table 122 Configure a manual aggregation group

Operation	Command	Description
Add a group of ports to a new manual aggregation group	**link-aggregation** *interface-type interface-number* **to** *interface-type interface-number* [**both**]	Optional
Configure a description for the aggregation group	**link-aggregation group** *agg-id* **description** *agg-name*	Optional By default, an aggregation group has no description.
Enter Ethernet port view	**interface** *interface-type interface-num*	-
Add the port to the aggregation group	**port link-aggregation group** *agg-id*	Required

Note that:

1. When creating an aggregation group:
   - If the aggregation group you are creating already exists but contains no port, its type will change to the type you set.
   - If the aggregation group you are creating already exists and contains ports, the possible type changes may be: changing from dynamic or static to manual, and changing from dynamic to static; and no other kinds of type change can occur.
   - When you change a dynamic/static group to a manual group, the system will automatically disable LACP on the member ports. When you change a dynamic/static group to a manual group, the system will remain the member ports LACP-enabled.
2. When a manual or static aggregation group contains only one port, you cannot remove the port unless you remove the whole aggregation group.

Configuring a Static LACP Aggregation Group

You can create a static LACP aggregation group, or remove an existing static aggregation group (after that, the system will re-aggregate the original member ports in the group to form one or more dynamic aggregation groups.).

You can manually add/remove a port to/from a static aggregation group, and a port can only be manually added/removed to/from a static aggregation group.

Table 123 Configure a static LACP aggregation group

Operation	Command	Description
Enter system view	**system-view**	-
Create a static aggregation group	**link-aggregation group** *agg-id* **mode static**	Required
Configure a description for the aggregation group	**link-aggregation group** *agg-id* **description** *agg-name*	Optional By default, an aggregation group has no description.
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Add the port to the aggregation group	**port link-aggregation group** *agg-id*	Required

For a static LACP aggregation group or a manual aggregation group, you are recommended not to cross cables between the two devices at the two ends of the aggregation group. For example, suppose port 1 of the local device is connected to port 2 of the peer device. To avoid cross-connecting cables, do not connect port 2 of the local device to port 1 of the peer device. Otherwise, packets may be lost.

Note that:

- LACP cannot be enabled on an existing port in a manual aggregation group.
- You can add a LACP-enabled port to a manual aggregation group. In this case, the system will disable LACP on the port automatically. Similarly, when you add a LACP-disabled port to a static aggregation group, the system will enable LACP on the port automatically.

Configuring a Dynamic LACP Aggregation Group

A dynamic LACP aggregation group is automatically created by the system based on LACP-enabled ports. The adding and removing of ports to/from a dynamic aggregation group are automatically accomplished by LACP.

You need to enable LACP on the ports whom you want to participate in dynamic aggregation of the system, because, only when LACP is enabled on those ports at both ends, can the two parties reach agreement in adding/removing ports to/from dynamic aggregation groups.

Enabling LACP on a member port of a manual aggregation group will not take effect.

Table 124 Configure a dynamic LACP aggregation group

Operation	Command	Description
Enter system view	**system-view**	-
Configure a description for an aggregation group	**link-aggregation group** *agg-id* **description** *agg-name*	Optional By default, an aggregation group has no description.
Configure the system priority	**lacp system-priority** *system-priority*	Optional By default, the system priority is 32,768.
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Enable LACP on the port	**lacp enable**	Required By default, LACP is disabled on a port.
Configure the port priority	**lacp port-priority** *port-priority*	Optional By default, the port priority is 32,768.

- If an existing aggregation group contains no port, the type of the aggregation group is set to the latest set type.
- If an aggregation group contains ports, you can only change a dynamic aggregation group or static aggregation group into a manual aggregation group, or change a dynamic aggregation group into a static aggregation group.

- When a dynamic aggregation group or a static aggregation group is changed into a manual aggregation group, the system will disable LACP on all the member ports automatically. When a dynamic aggregation group is changed into a static aggregation group, LACP on all the member ports remains enabled.

Note that if a manual aggregation group or a static aggregation group contains only one port, this port cannot be removed from the aggregation group. Instead, it can be removed from the aggregation group only in the way of removing the aggregation group.



*If you use the **save** command to save the current configuration and then restart the device, the configured manual/static aggregation groups and their descriptions still exist, however, the dynamic aggregation groups will disappear and their descriptions cannot be restored.*

Configuring Parameters for HASH

Through the following configuration tasks, you can configure parameters used by the HASH algorithm in link aggregation, thus controlling load balancing on aggregated ports effectively.

Table 125 Configure parameters for HASH

Operation	Command	Description
Enter system view	**system-view**	-
Configure parameters used by the HASH algorithm in link aggregation	**hash** { **dstip** | **dstmac** | **ip** | **l4port** | **mac** | **srcip** | **srcmac** } { **ioboard slot** *slot-number* | **mainboard** }	By default, Type A I/O Modules use four-tuple (**dstip**, **dstmac**, **srcip** and **srcmac**) as the parameter of HASH algorithm. I/O Modules other than Type A use **ip** as the parameter of HASH algorithm.



- *All the seven parameters are available on type-A I/O Modules including 3C16860, 3C16860, 3C16861, 3C16861, LS81FS24A, LS81FS24, 3C16858, 3C16858, 3C16859, and 3C16859.*
- *None of the above seven parameters are available on non-type-A I/O Modules.*
- *Only type-A I/O Modules support **l4port**.*

Displaying and Maintaining Link Aggregation Configuration

After the above configuration, execute the **display** command in any view to display the running status after the link aggregation configuration and verify your configuration.

Execute the **reset** command in user view to clear LACP statistics on ports.

Table 126 Display and maintain link aggregation configuration

Operation	Command
Display summary information of all aggregation groups	**display link-aggregation summary**
Display detailed information of a specific aggregation group or all aggregation groups	**display link-aggregation verbose** *agg-id*

Table 126 Display and maintain link aggregation configuration

Operation	Command
Display the ID of the local device	**display lacp system-id**
Display link aggregation details of a specified port or port range	**display link-aggregation interface** *interface-type interface-number* | [**to** *interface-type interface-number*]
Clear LACP statistics about a specified port or port range	**reset lacp statistics** [**interface** *interface-type interface-number* [**to** *interface-type interface-number*]]

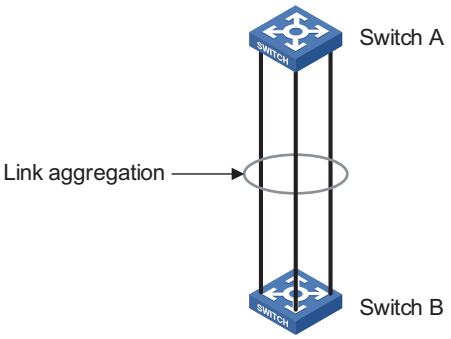
Link Aggregation Configuration Example

Network requirements

- Switch A connects to Switch B with three ports Ethernet 2/0/1 to Ethernet 2/0/3. It is required that incoming/outgoing load between the two switch can be shared among the three ports.
- Adopt three different aggregation modes to implement link aggregation on the three ports between switch A and B.

Network diagram

Figure 51 Network diagram for link aggregation configuration



Configuration procedure

The following only lists the configuration on Switch A; you must perform the similar configuration on Switch B to implement link aggregation.

1 Adopt the manual aggregation mode

Create manual aggregation group 1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z
[SW7750] link-aggregation group 1 mode manual
```

Add Ethernet 2/0/1 through Ethernet 2/0/3 to aggregation group 1.

```
[SW7750] interface ethernet2/0/1
[SW7750-Ethernet2/0/1] port link-aggregation group 1
[SW7750-Ethernet2/0/1] interface ethernet2/0/2
[SW7750-Ethernet2/0/2] port link-aggregation group 1
[SW7750-Ethernet2/0/2] interface ethernet2/0/3
[SW7750-Ethernet2/0/3] port link-aggregation group 1
```

2 Adopt the static LACP aggregation mode

Create static aggregation group 1.

```
[SW7750] link-aggregation group 1 mode static
```

Add Ethernet 2/0/1 through Ethernet 2/0/3 to aggregation group 1.

```
[SW7750] interface ethernet2/0/1
[SW7750-Ethernet2/0/1] port link-aggregation group 1
[SW7750-Ethernet2/0/1] interface ethernet2/0/2
[SW7750-Ethernet2/0/2] port link-aggregation group 1
[SW7750-Ethernet2/0/2] interface ethernet2/0/3
[SW7750-Ethernet2/0/3] port link-aggregation group 1
```

3 Adopt the dynamic LACP aggregation mode

Enable LACP on Ethernet 2/0/1 through Ethernet 2/0/3.

```
[SW7750] interface ethernet2/0/1
[SW7750-Ethernet2/0/1] lacp enable
[SW7750-Ethernet2/0/1] interface ethernet2/0/2
[SW7750-Ethernet2/0/2] lacp enable
[SW7750-Ethernet2/0/2] interface ethernet2/0/3
[SW7750-Ethernet2/0/3] lacp enable
```

Note that the three LACP-enabled ports can be aggregated into a dynamic aggregation group to implement load sharing only when they have the same basic configuration, rate and duplex mode.

24 PORT ISOLATION CONFIGURATION

Port Isolation Overview

Introduction to Port Isolation

Through the port isolation feature, you can add the ports to be controlled into an isolation group to isolate Layer 2 and Layer 3 data between ports in the isolation group. Thus, it can improve network security and deliver flexible networking solutions.

Currently, you can configure 64 isolation groups on a switch. The number of Ethernet ports an isolation group can accommodate is not limited.



- *An isolation group only isolates the member ports in it.*
- *The port isolation function is independent of VLAN configuration.*

Port Isolation and Link Aggregation

- When a port in an aggregation group joins an isolation group, the other ports in the aggregation group join the isolation group automatically.
- When a port in an aggregation group leaves an isolation group, the other ports in the aggregation group leave the isolation group automatically.

Configuring Port Isolation

Table 127 lists the operations to add an Ethernet port to an isolation group to isolate Layer 2 data between ports in the isolation group.

Table 127 Configure port isolation

Operation	Command	Description
Enter system view	**system-view**	-
Create an isolation group	**port-isolate group** *group-id*	Required
Specify a description string for the current isolation group	**description** *text*	Optional
Add the specified port into the isolation group	**port** *interface-list*	Optional By default, an isolation group contains no Ethernet port.
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Add the current Ethernet port to the specified isolation group	**port isolate group** *group-id*	Optional By default, an isolation group contains no Ethernet port.

- *An Ethernet port belongs to only one port isolation group. If you add an Ethernet port to different isolation groups, the port belongs to only the latest isolation group to which the port is added.*
- *Currently, modules of Type A (3C16860, 3C16861, LS81FS24A, 3C16858, and 3C16859) do not support the Port Isolation feature.*

Displaying Port Isolation Configuration

After the above configuration, you can execute the **display** command in any view to view the information about the Ethernet ports added to an isolation group.

Table 128 Display port isolation configuration

Operation	Command
Display the configuration of the created isolation group	**display isolate port** [**group** *group-id*]

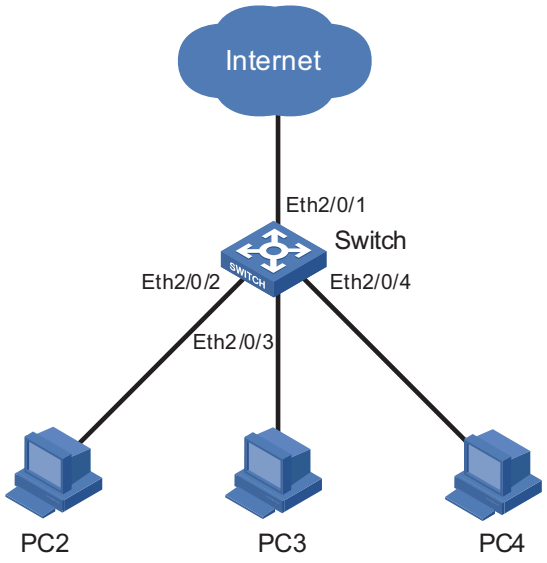
Port Isolation Configuration Example

Network requirements

- PC2, PC3 and PC4 connect to the switch ports Ethernet2/0/2, Ethernet2/0/3, and Ethernet2/0/4 respectively.
- It is desired that PC2, PC3 and PC4 are isolated from each other so that they cannot communicate with each other.

Network diagram

Figure 52 Network diagram for port isolation configuration



Configuration procedure

Create isolation group 1.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] port-isolate group 1
```

Add Ethernet2/0/2, Ethernet2/0/3, and Ethernet2/0/4 to the isolation group 1.

```
[SW7750-port-isolate-group1] port Ethernet2/0/2 to Ethernet2/0/4
```

Display information about the ports in the isolation group.

```
[SW7750-port-isolate-group1] display isolate port
 Isolate group ID: 1
 Isolated port(s) in group 1:
             Ethernet2/0/2  Ethernet2/0/3  Ethernet2/0/4
```

25 PORT SECURITY CONFIGURATION

Currently, A type modules (3C16860, 3C16860, 3C16861, 3C16861, LS81FS24A, LS81FS24, 3C16858, 3C16858, 3C16859, and 3C16859) do not support the port security feature.

Port Security Overview

Introduction

Port security is a security mechanism for network access control. It is an expansion to the current 802.1x and MAC address authentication.

Port security defines various security modes that allow devices to learn legal source MAC addresses, in order for you to implement different network security management as needed. With port security, packets whose source MAC addresses cannot be learned by your switch in a security mode are considered illegal packets, and 802.1x authentication failure events and MAC authentication failure events are considered illegal events.

Upon detecting an illegal packet or illegal event, the system triggers the corresponding port security features and takes pre-defined actions automatically. This reduces your maintenance workload and greatly enhances system security and manageability.

Port Security Features

The following port security features are provided:

1. NTK (need to know) feature: By checking the destination MAC addresses in outbound data frames on a port, NTK ensures that only successfully authenticated devices can obtain data frames from the port, thus preventing illegal devices from intercepting network data.
2. Intrusion protection feature: By checking the source MAC addresses in inbound data frames or the username and password in 802.1x authentication requests on a port, intrusion protection detects illegal packets (packets with illegal MAC address) or events and takes a pre-set action accordingly. The actions you can set include: disconnecting the port temporarily/permanently, and blocking packets with invalid MAC addresses.
3. Device tracking feature: When special data packets (generated from illegal intrusion, abnormal login/logout or other special activities) are passing through a switch port, device tracking enables the switch to send Trap messages to help the network administrator monitor special activities.

Port Security Modes

Table 129 describes the available port security modes:

Table 129 Description of port security modes

Security mode	Description	Feature
autolearn	In this mode, the port automatically learns MAC addresses and changes them to security MAC addresses. This security mode will automatically change to the **secure** mode after the amount of security MAC addresses on the port reaches the maximum number configured with the **port-security max-mac-count** command. After the port security mode is changed to the **secure** mode, only those packets whose source MAC addresses are security MAC addresses learned configured can pass through the port.	In the secure mode, the device will trigger NTK and intrusion protection upon detecting an illegal packet.
secure	In this mode, the port is disabled from learning MAC addresses. Only those packets whose source MAC addresses are static MAC addresses configured can pass through the port.	
userlogin	In this mode, port-based 802.1x authentication is performed for access users.	In this mode, neither NTK nor intrusion protection will be triggered.

Table 129 Description of port security modes

Security mode	Description	Feature
userlogin-secure	The port is enabled only after an access user passes the MAC-based 802.1x authentication. When the port is enabled, only the packets of the successfully authenticated user can pass through the port. In this mode, only one 802.1x-authenticated user is allowed to access the port. When the port changes from the normal mode to this security mode, the system automatically removes the existing dynamic MAC address entries and authenticated MAC address entries on the port.	In any of these modes, the device will trigger NTK and intrusion protection upon detecting an illegal packet.
userlogin-secure-ext	This mode is similar to the **userlogin-secure** mode, except that there can be more than one 802.1x-authenticated user on the port.	
userlogin-secure-oui	This mode is similar to the **userlogin-secure** mode, except that, besides the packets of the single 802.1x-authenticated user, the packets whose source MAC addresses have a particular OUI are also allowed to pass through the port. When the port changes from the normal mode to this security mode, the system automatically removes the existing dynamic/authenticated MAC address entries on the port.	
macAddressWithRadius	In this mode, MAC address-based authentication is performed for access users.	
userlogin-secure-or-mac	In this mode, the two kinds of authentication in **macAddressWithRadius** and **userlogin-secure** modes can be performed simultaneously. In this mode, there can be only one authenticated 802.1x user on the port.	
userlogin-secure-or-mac-ext	This mode is similar to the **userlogin-secure-or-mac** mode, except that there can be more than one authenticated 802.1x user on the port.	
mac-else-userlogin-secure	MAC authentication is performed first on the accessing user. If the MAC authentication succeeds, the access user has the accessibility; otherwise, 802.1x authentication is performed on the access user. In this mode, there can be only one authenticated 802.1x user on the port.	
mac-else-userlogin-secure-ext	This mode is similar to the **mac-else-userlogin-secure** mode, except that there can be more than one authenticated 802.1x user on the port.	

- *When a port works in the **mac-else-userlogin-secure** mode or the **mac-else-userlogin-secure-ext** mode, for the same packet, intrusion protection can be triggered only after both MAC authentication and 802.1x authentication fail.*
- *When a port works in the **userlogin-secure-oui** mode, intrusion protection will not be triggered even if the port receives a frame with an OUI value that is not the specified one.*

Port Security Configuration

Table 130 Port security configuration tasks

Task		Remarks
"Enabling Port Security" on page 202		Required
"Setting the Maximum Number of MAC Addresses Allowed on a Port" on page 202		Optional
"Setting the Port Security Mode" on page 203		Required
"Configuring Port Security Features" on page 204	"Configuring the NTK feature" on page 204	Optional Choose one or more features as required.
	"Configuring intrusion protection" on page 204	
	"Configuring the Trap feature" on page 204	
"Ignoring the Authorization Information from the RADIUS Server" on page 204		Optional
"Configuring Security MAC Addresses" on page 205		Optional

Enabling Port Security

Table 131 Enable port security

Operation	Command	Remarks
Enter system view	**system-view**	-
Enable port security	**port-security enable**	Required Disabled by default

CAUTION: *Enabling port security resets the following configurations on the ports to the defaults (shown in parentheses below)*

- *802.1x (disabled), port access control method (**macbased**), and port access control mode (**auto**)*
- *MAC authentication (disabled)*

In addition, you cannot perform the above-mentioned configurations manually because these configurations change with the port security mode automatically.

- *For details about 802.1x configuration, refer to "802.1x Configuration" on page 389.*
- *For details about MAC authentication configuration, refer to "Centralized MAC Address Authentication Configuration" on page 233.*

Setting the Maximum Number of MAC Addresses Allowed on a Port

Port security allows more than one user to be authenticated on a port. The number of authenticated users allowed, however, cannot exceed the configured upper limit.

By setting the maximum number of MAC addresses allowed on a port, you can

- Control the maximum number of users who are allowed to access the network through the port
- Control the number of Security MAC addresses that can be added with port security

This configuration is different from that of the maximum number of MAC addresses that can be leaned by a port in MAC address management.

Table 132 Set the maximum number of MAC addresses allowed on a port

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Set the maximum number of MAC addresses allowed on the port	**port-security max-mac-count** *count-value*	Required Not limited by default

Setting the Port Security Mode

Table 133 Set the port security mode

Operation	Command	Remarks
Enter system view	**system-view**	-
Set the OUI value for user authentication	**port-security oui** *OUI-value* **index** *index-value*	Optional In **userlogin-secure-oui** mode, a port supports one 802.1x user plus one user whose source MAC address has a specified OUI value.
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Set the port security mode	**port-security port-mode** { **autolearn** | **mac-authentication** | **mac-else-userlogin-secure** | **mac-else-userlogin-secure-ext** | **secure** | **userlogin** | **userlogin-secure** | **userlogin-secure-ext** | **userlogin-secure-or-mac** | **userlogin-secure-or-mac-ext** | **userlogin-withoui** }	Required By default, a port operates in normal mode. You can set a port security mode as needed.

- *Before setting the port security mode to **autolearn**, you need to set the maximum number of MAC addresses allowed on the port with the **port-security max-mac-count** command.*
- *After you set the port security mode to **autolearn**, you cannot configure any static or blackhole MAC addresses on the port.*
- *To change the security mode of a port that is not in the normal forwarding state, you need to perform the **undo port-security port-mode** command or disable port security at first.*

If the **port-security port-mode** *mode* command has been executed on a port, none of the following can be configured on the same port:

- Maximum number of MAC addresses that the port can learn
- Disabling MAC address learning
- Reflector port for port mirroring
- Link aggregation

- Voice VLAN

Configuring Port Security Features

Configuring the NTK feature

Table 134 Configure the NTK feature

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Configure the NTK feature	**port-security ntk-mode** { **ntkonly** | **ntk-withbroadcasts** | **ntk-withmulticasts** }	Required Be default, NTK is disabled on a port, namely all frames are allowed to be sent.

Configuring intrusion protection

Table 135 Configure the intrusion protection feature

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Set the corresponding action to be taken by the switch when intrusion protection is triggered	**port-security intrusion-mode** { **disablepo rt** | **disableport-temporarily** | **blockmac** }	Required By default, intrusion protection is not configured.
Return to system view	**quit**	-
Set the timer during which the port remains disabled	**port-security timer disableport** *timer*	Optional 20 seconds by default

*The **port-security timer disableport** command is used in conjunction with the **port-security intrusion-mode disableport-temporarily** command to set the length of time during which the port remains disabled.*

Configuring the Trap feature

Table 136 Configure port security trapping

Operation	Command	Remarks
Enter system view	**system-view**	-
Enable sending traps for the specified type of event	**port-security trap** { **addresslearned** | **intrusion** | **dot1xlogon** | **dot1xlogoff** | **dot1xlogfailure** | **ralmlogon** | **ralmlogoff** | **ralmlogfailure** }	Required By default, no trap is sent.

Ignoring the Authorization Information from the RADIUS Server

After an 802.1x user or MAC-authenticated user passes Remote Authentication Dial-In User Service (RADIUS) authentication, the RADIUS server delivers the authorization information to the device. You can configure a port to ignore the authorization information from the RADIUS server.

Table 137 Configure a port to ignore the authorization information from the RADIUS server

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Ignore the authorization information from the RADIUS server	**port-security authorization ignore**	Required By default, a port uses the authorization information from the RADIUS server.

Configuring Security MAC Addresses

Security MAC addresses are special MAC addresses that never age out. One security MAC address can be added to only one port in the same VLAN so that you can bind a MAC address to one port in the same VLAN.

Security MAC addresses can be learned by the auto-learn function of port security or manually configured.

Before adding security MAC addresses to a port, you must configure the port security mode to **autolearn**. After this configuration, the port changes its way of learning MAC addresses as follows.

- The port deletes original dynamic MAC addresses;
- If the amount of security MAC addresses has not yet reach the maximum number, the port will learn new MAC addresses and turn them to security MAC addresses;
- If the amount of security MAC addresses reaches the maximum number, the port will not be able to learn new MAC addresses and the port mode will be changed from **autolearn** to **secure**.



The security MAC addresses manually configured are written to the configuration file; they will not get lost when the port is up or down. As long as the configuration file is saved, the security MAC addresses can be restored after the switch reboots.

Configuration prerequisites

- Port security is enabled.
- The maximum number of security MAC addresses allowed on the port is set.
- The security mode of the port is set to **autolearn**.

Configuring a security MAC address

Table 138 Configure a security MAC address

Operation	Command	Remarks
Enter system view	**system-view**	-
Add a security MAC address	**mac-address security** *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*	Required. By default, no security MAC address is configured.

Displaying Port Security Configuration

After the above configuration, you can use the **display** command in any view to display port security information and verify your configuration.

Table 139 Display port security configuration

Operation	Command	Description
Display information about port security configuration	**display port-security** [**interface** *interface-list*]	You can execute the **display** command in any view.
Display information about security MAC address configuration	**display mac-address security** [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**]	

Port Security Configuration Example

Port Security Configuration Example

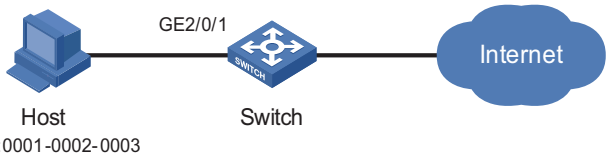
Network requirements

Implement access user restrictions through the following configuration on GigabitEthernet 2/0/1 of the switch.

- Allow a maximum of 80 users to access the port without authentication and permit the port to learn and add the MAC addresses of the users as security MAC addresses.
- To ensure that Host can access the network, add the MAC address 0001-0002-0003 of Host as a security MAC address to the port in VLAN 1.
- After the number of security MAC addresses reaches 80, the port stops learning MAC addresses. If any frame with an unknown MAC address arrives, intrusion protection is triggered and the port will be disabled and stay silent for 30 seconds.

Network diagram

Figure 53 Network diagram for port security configuration



Configuration procedure

Enter system view.

```
<SW7750> system-view
```

Enable port security.

```
[SW7750] port-security enable
```

Enter GigabitEthernet 2/0/1 port view.

```
[SW7750] interface GigabitEthernet 2/0/1
```

Set the maximum number of MAC addresses allowed on the port to 80.

```
[SW7750-GigabitEthernet2/0/1] port-security max-mac-count 80
```

Set the port security mode to **autolearn**.

```
[SW7750-GigabitEthernet2/0/1] port-security port-mode autolearn
[SW7750-GigabitEthernet2/0/1] quit
```

Add the MAC address 0001-0002-0003 of Host as a security MAC address to the port in VLAN 1.

```
[SW7750] mac-address security 0001-0002-0003 interface GigabitEthern
et 2/0/1 vlan 1
```

Configure the port to be silent for 30 seconds after intrusion protection is triggered.

```
[SW7750-GigabitEthernet2/0/1] port-security intrusion-mode disablepo
rt-temporarily
[SW7750-GigabitEthernet2/0/1] quit
[SW7750] port-security timer disableport 30
```

26 PORT BINDING CONFIGURATION

Currently, A type modules (3C16860, 3C16860, 3C16861, 3C16861, LS81FS24A, LS81FS24, 3C16858, 3C16858, 3C16859, and 3C16859) do not support the port binding feature.

Port Binding Overview

Introduction

Port binding enables the network administrator to bind the MAC address and IP address of a user with a specific port. After the binding, the switch forwards only the packets received on the port whose MAC address and IP address are identical with the bound MAC address and IP address. This improves network security and enhances security monitoring.

Configuring Port Binding

Table 140 Configure port binding

Operation	Command		Description
Enter system view	**system-view**		-
Bind the MAC address and IP address of a legal user with a specific port	In system view	**am user-bind** { **mac-addr** *mac-address* | **ip-addr** *ip-address* }* *interface-list*	Either is required. By default, the MAC and IP addresses of a user is not bound with any port.
	In Ethernet port view	**interface** *interface-type interface-number*	
		am user-bind { **mac-addr** *mac-address* | **ip-addr** *ip-address* }*	

Displaying Port Binding Configuration

After the above configuration, you can use the **display** command in any view to display port binding information and verify your configuration.

Table 141 Display port binding configuration

Operation	Command	Description
Display port binding information	**display am user-bind** [**interface** *interface-type interface-number* | **mac-addr** *mac-address* | **ip-addr** *ip-address*]	You can execute the **display** command in any view.

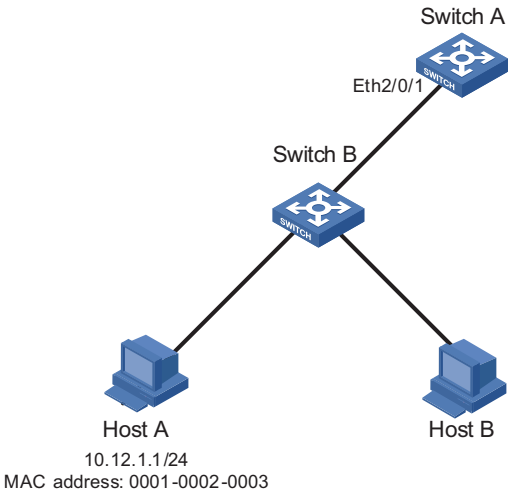
Port Binding Configuration Example

Network requirements

It is required to bind the MAC and IP addresses of Host A to Ethernet 2/0/1 on switch A, so that Ethernet 2/0/1 can only forward packets coming from or going to Host A.

Network diagram

Figure 54 Network diagram for port binding configuration



Configuration procedure

Configure switch A as follows:

Enter system view.

```
<SW7750> system-view
```

Enter Ethernet 2/0/1 port view.

```
[SW7750] interface Ethernet2/0/1
```

Bind the MAC address and the IP address of Host A to Ethernet 2/0/1.

```
[SW7750-Ethernet2/0/1] am user-bind mac-addr 0001-0002-0003 ip-addr 10.12.1.1
```

27 DLDP CONFIGURATION

Overview

Introduction

You may have encountered unidirectional links in networking. When a unidirectional link occurs, the local device can receive packets from the peer device through the link layer, but the peer device cannot receive packets from the local device. Unidirectional link can cause problems such as spanning tree protocol (STP) loops.

Unidirectional links can be caused by

- Fiber cross-connection, as shown in Figure 55
- Fibers that are not connected or disconnected, as shown in Figure 56, the hollow lines in which refer to fibers that are not connected or disconnected.

Device link detection protocol (DLDP) can detect the link status of an optical fiber cable or copper twisted pair (such as super category 5 twisted pair). If DLDP finds a unidirectional link, it disables the related port automatically or prompts you to disable it manually according to the configurations, to avoid network problems.

Figure 55 Fiber cross-connection

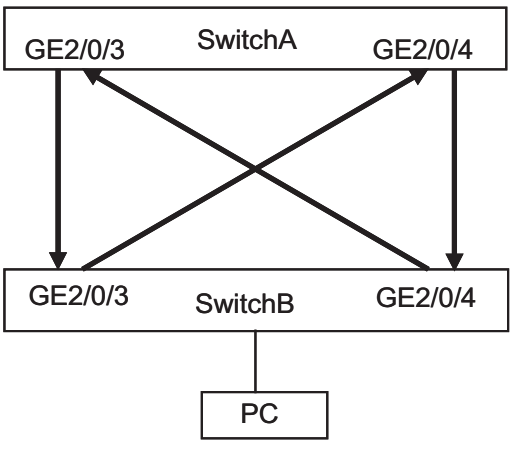
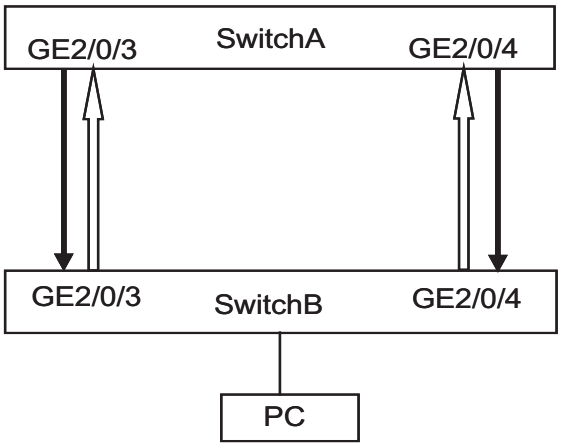


Figure 56 Fiber broken or not connected



DLDP provides the following features:

- As a link layer protocol, it works together with the physical layer protocols to monitor the link status of a device.
- The auto-negotiation mechanism at the physical layer detects physical signals and faults. DLDP identifies peer devices and unidirectional links, and disables unreachable ports.
- Even if both ends of links can work normally at the physical layer, DLDP can detect whether these links are connected correctly and whether packets can be exchanged normally at both ends. However, the auto-negotiation mechanism cannot implement this detection.

- *In order for DLDP to detect fiber disconnection in one direction, you need to configure the port to work in mandatory full duplex mode at a mandatory rate.*
- *When the port determines the duplex mode and speed through auto-negotiation, even if DLDP is enabled, it does not take effect when the fiber in one direction is disconnected. In this case, the port is considered down.*

DLDP Fundamentals

DLDP Implementation

DLDP detects link status by exchanging the following types of packets.

Table 142 DLDP packet types

DLDP packet type	Function
Advertisement	Notifies the neighbor devices of the existence of the local device. An advertisement packet carries only the local port information, and it does not require response from the peer end.
RSY-Advertisement packets (referred to as RSY packets hereafter)	Advertisement packet with the RSY flag set to 1. RSY advertisement packets are sent to request synchronizing the neighbor information when neighbor information is not locally available or a neighbor information entry ages out.
Flush-Advertisement packets (referred to as flush packets hereafter)	Advertisement packet with the flush flag set to 1. A flush packet carries only the local port information (instead of the neighbor information) and is used to trigger neighbors to remove the information about the local device.
Probe	Probe packets are used to probe the existence of a neighbor. Echo packets are required from the corresponding neighbor. Probe packets carry the local port information. Neighbor information is optional for probe packets. A probe packet carrying neighbor information probes the specified neighbors; A probe packet carrying no neighbor information probes all the neighbors.
Echo	Response to probe packets. An echo packet carries the information about the response port and the neighbor information it maintains. Upon receiving an echo packet, a port checks whether the neighbor information carried in the echo packet is consistent with that of itself. If yes, the link between the local port and the neighbor is regarded as bidirectional.
Disable	Disable packets are used to notify the peer end that the local end is in the disable state. Disable packets carry only the local port information instead of the neighbor information. When a port detects a unidirectional link and enters the disable state, the port sends disable packets to the neighbor. A port enters the disable state upon receiving a disable packet.
LinkDown	Linkdown packets are used to notify unidirectional link emergencies (a unidirectional link emergency occurs when the local port is down and the peer port is up). Linkdown packets carry only the local port information instead of the neighbor information. In some conditions, a port is considered to be physically down if the link connecting to the port is physically abnormal (for example, the Rx line of the fiber on the port is disconnected, while the Tx line operates properly). But for the peer end, as Rx signals can still be received on the physical layer, the port is still considered to be normal. Such a situation is known as unidirectional link emergency. When a unidirectional link emergency occurs, DLDP sends linkdown packets immediately to inform the peer of the link abnormality. Without linkdown packets, the peer can detect the link abnormality only after a period when the corresponding neighbor information maintained on the neighbor device ages out, which is three times the advertisement interval. Upon receiving a linkdown packet, if the peer end operates in the enhanced mode, it enters the disable state, and sets the receiving port to the DLDP down state (auto shutdown mode) or gives an alarm to the user (manual shutdown mode).
Recover Probe	Recover probe packets are used to detect whether a link recovers to implement the port auto-recovery mechanism. Recover probe packets carry only the local port information instead of the neighbor information. They request for recover echo packets as the response. A port in the DLDP down state sends a recover probe packet every two seconds.

Table 142 DLDP packet types

DLDP packet type	Function
Recover Echo	Recover echo packets are response to recover probe packets in the port auto-recovery mechanism. A link is considered to restore to the bidirectional state if a port on one end sends a recover probe packet, receives a recover echo packet, and the neighbor information contained in the recover echo packet is consistent with that of the local port.

1 If the DLDP-enabled link is up, DLDP sends DLDP packets to the peer device, and analyzes/processes the DLDP packets received from the peer device. DLDP packets sent in different DLDP states are of different types.

Table 143 DLDP state and DLDP packet type

DLDP state	Type of the DLDP packets sent
Active	Advertisement packets, with the RSY flag set or not set.
Advertisement	Advertisement packets
Probe	Probe packets

2 A DLDP packet received is processed as follows:

- In authentication mode, the DLDP packet is authenticated and is then dropped if it fails the authentication.
- The packet is further processed, as described in Table 144.

Table 144 The procedure to process a received DLDP packet

Packet type	Processing procedure				
Advertisement packet	Extracts neighbor information		If the corresponding neighbor entry does not exist on the local device, DLDP creates the neighbor entry, triggers the entry aging timer, and switches to the probe state.		
			If the corresponding neighbor entry already exists on the local device, DLDP resets the aging timer of the entry.		
Flush packet	Removes the neighbor entry from the local device				
Probe packet	Sends echo packets containing both neighbor and its own information to the peer		Creates the neighbor entry if it does not exist on the local device.		
			Resets the aging timer of the entry if the neighbor entry already exists on the local device.		
Echo packet	Checks to see if the local device is in the probe state	No	Drops the echo packet		
		Yes	Checks to see if the neighbor information contained in the packet is the same as that on the local device	No	Drops the echo packet
				Yes	Sets the flag bit of the neighbor to bidirectional link
					If all neighbors are in the bidirectional link state, DLDP switches from the probe state to the advertisement state, and sets the echo waiting timer to 0.

3 If no echo packet is received from the neighbor, DLDP performs the following processing:

Table 145 Processing procedure when no echo packet is received from the neighbor

No echo packet received from the neighbor	Processing procedure
In normal mode, no echo packet is received when the echo waiting timer expires.	DLDP switches to the **disable** state, outputs log and tracking information, and sends flush packets. Depending on the user-defined DLDP down mode, DLDP disables the local port automatically or prompts you to disable the port manually. DLDP sends RSY messages and removes the corresponding neighbor entries.
In enhanced mode, no echo packet is received when the enhanced timer expires	

DLDP Status

A link can be in one of these DLDP states: initial, inactive, active, advertisement, probe, disable, and delaydown.

Table 146 DLDP status

Status	Description
Initial	Initial status before DLDP is enabled.
Inactive	DLDP is enabled but the corresponding link is down
Active	DLDP is enabled, and the link is up or an neighbor entry is cleared
Advertisement	All neighbors communicate normally in both directions, or DLDP remains in active state for more than five seconds and enters this status. It is a stable state where no unidirectional link is found
Probe	DHCP sends packets to check whether the link is a unidirectional. It enables the probe sending timer and an echo waiting timer for each target neighbor.
Disable	DLDP detects a unidirectional link, or finds (in enhanced mode) that a neighbor disappears. In this case, DLDP sends and receives only recover probe packets and recover echo packets.
DelayDown	When a device in the active, advertisement, or probe DLDP state receives a port down message, it does not removes the corresponding neighbor immediately, neither does it changes to the inactive state. Instead, it changes to the delaydown state first. When a device changes to the delaydown state, the related DLDP neighbor information remains, and the DelayDown timer is triggered. After the DelayDown timer expires, the DLDP neighbor information is removed.

DLDP Timers

Table 147 DLDP timers

Timer	Description
Advertisement sending timer	Interval between sending advertisement packets, which can be configured on a command line interface. By default, the timer length is 5 seconds.
Probe sending timer	The interval is 0.5 seconds. In the probe state, DLDP sends two probe packets in a second.

Table 147 DLDP timers

Timer	Description
Echo waiting timer	It is enabled when DLDP enters the probe state. The echo waiting timer length is 10 seconds.
	If no echo packet is received from the neighbor when the Echo waiting timer expires, the state of the local end is set to unidirectional link (one-way audio) and the state machine turns into the **disable** state. DLDP outputs log and tracking information, sends flush packets. Depending on the user-defined DLDP down mode, DLDP disables the local port automatically or prompts you to disable the port manually. At the same time, DLDP deletes the neighbor entry.
Entry aging timer	When a new neighbor joins, a neighbor entry is created and the corresponding entry aging timer is enabled
	When an advertisement packet is received from a neighbor, the neighbor entry is updated and the corresponding entry aging timer is updated
	In the normal mode, if no packet is received from the neighbor when the entry aging timer expires, DLDP sends an advertisement packet with an RSY tag, and deletes the neighbor entry.
	In the enhanced mode, if no packet is received from the neighbor when the entry aging timer expires, DLDP enables the enhanced timer
	The entry aging timer length is three times the advertisement timer length.
Enhanced timer	In the enhanced mode, if no packet is received from the neighbor when the entry aging timer expires, DLDP enables the enhanced timer for the neighbor. The enhanced timer length is 10 seconds
	The enhanced timer then sends one probe packet every second and eight packets successively to the neighbor.
	If no echo packet is received from the neighbor when the enhanced timer expires, the state of the local end is set to unidirectional communication state and the state machine turns into the **disable** state. DLDP outputs log and tracking information and sends flush packets. Depending on the user-defined DLDP down mode, DLDP disables the local port automatically or prompts you to disable the port manually. Meanwhile, DLDP deletes the neighbor entry.

Table 147 DLDP timers

Timer	Description
DelayDown timer	When a device in the active, advertisement, or probe DLDP state receives a port down message, it does not removes the corresponding neighbor immediately, neither does it changes to the inactive state. Instead, it changes to the delaydown state first. When a device changes to the delaydown state, the related DLDP neighbor information remains, and the DelayDown timer is triggered. The DelayDown timer is configurable and ranges from 1 to 5 seconds. A device in the delaydown state only responds to port up messages. A device in the delaydown state resumes its original DLDP state if it receives a port up message before the delaydown timer expires. Otherwise, it removes the DLDP neighbor information and changes to the inactive state.

DLDP Operating Mode

DLDP can operate in two modes: normal and enhanced.

Table 148 DLDP operating mode and neighbor entry aging

DLDP operating mode	DLDP detects whether neighbors exist or not when neighbor tables are aging	The entry aging timer is enabled or not during neighbor entry aging	The enhanced timer is enabled or not when the entry aging timer expires
Normal mode	No	Yes (The neighbor entry ages out after the entry aging timer expires)	No
Enhanced mode	Yes	Yes (The enhanced timer is enabled after the entry aging timer expires)	Yes (When the enhanced timer expires, the state of the local end is set to unidirectional link, and the neighbor entry is aged out.)

DLDP Neighbor State

A DLDP neighbor can be in one of these two states: two way and unknown. You can check the state of a DLDP neighbor by using the **display dldp** command.

Table 149 Description on the two DLDP neighbor states

DLDP neighbor state	Description
two way	The link to the neighbor operates properly.
unknown	The device is detecting the neighbor and the neighbor state is unknown.

Link Auto-recovery Mechanism

If the shutdown mode of a port is set to auto shutdown, the port is set to the DLDP down state when DLDP detects the link connecting to the port is a unidirectional link. A port in DLDP down state does not forward service packets or receive/send protocol packets except DLDPDUs.

A port in the DLDP down state recovers when the corresponding link recovers. A port in the DLDP down state sends recover probe packets periodically. On receiving a correct recover echo packet (which means that the unidirectional link is restored to a bidirectional link), it is brought up by DLDP. The detailed process is as follows.

1. A port in the DLDP down state sends a recover probe packet every 2 seconds. Recover probe packets carry only the local port information.
2. Upon receiving a recover probe packet, the peer end responds with a recover echo packet.
3. Upon receiving a recover echo packet, the local end checks to see if the neighbor information carried in the recover echo packet is consistent with that of the local port. If yes, the link between the local port and the neighbor is considered to be recovered to bidirectional, the port changes from the disable state to the active state, and neighboring relationship is reestablished between the local port and the neighbor.



Only ports in the DLDP down state can send and process recover probe packets and recover echo packets. The auto-recovery mechanism does apply to ports that are shut down manually.

DLDP Configuration

Configuring DLDP



*For a port with DLDP enabled, you are not recommended to execute the **port monitor last** command on the port. If it is necessary, the value argument in this command must be less than 10.*

The following table describes the DLDP configuration tasks:

Table 150 DLDP configuration tasks

Operation			Command	Description
Enter system view			**system-view**	-
Enable DLDP	Enable DLDP globally		**dldp enable**	Required.
	Enable DLDP on a port	Enter Ethernet port view	**interface** *interface-type interface-number*	Enable DLDP globally and then enable DLDP on the specified port.
		Enable DLDP on a port	**dldp enable**	

Table 150 DLDP configuration tasks

Operation	Command	Description
Set the authentication mode and password	**dldp authentication-mode** { **none** | **simple** *simple-password* | **md5** *md5-password* }	Optional By default, the authentication mode is **none**, that is, authentication is not performed.
Set the interval of sending DLDP packets	**dldp interval** *value*	Optional. By default, the interval of sending DLDP packets is 5 seconds.
Set the delaydown timer	**dldp delaydown-timer** *delaydown-time*	Optional By default, the delaydown timer expires after 1 second it is triggered.
Set the DLDP handling mode when an unidirectional link is detected	**dldp unidirectional-shutdown** { **auto** | **manual** }	Optional By default, the handling mode is auto
Set the operating mode of DLDP	**dldp work-mode** { **enhance** | **normal** }	Optional By default, DLDP works in normal mode.
Enter Ethernet port view	**interface** *interface-type interface-number*	-

Table 150 DLDP configuration tasks

Operation	Command	Description
Force the duplex attribute	**duplex full**	Required If you want to use DLDP to detect which fiber of the two fibers is not connected or fails, you must configure the ports to work in the mandatory full duplex mode.
Force the speed value	**speed** *speed-value*	Required
Display the configuration information about the DLDP-enabled ports	**display dldp** [*interface-type interface-number*]	-

- *When you use the **dldp enable/dldp disable** command in system view to enable/disable DLDP globally on all optical ports of the switch, this command is only valid for existing optical ports on the device, however, it is not valid for those added subsequently.*
- *DLDP can operate normally only when the same authentication mode and password are set for local and peer ports.*
- *When the DLDP protocol works in normal mode, the system can identify only one type of unidirectional links: cross-connected fibers.*
- *When the DLDP protocol works in enhanced mode, the system can identify two types of unidirectional links: the first type is the cross-connected fiber, and the second type is one of the two fibers is not connected or fails.*
- *When the device is busy with services and the CPU utilization is high, DLDP may issue mistaken reports. You are recommended to configure the operating mode of DLDP as manual after unidirectional links are discovered.*
- *For the **dldp interval** integer command, make sure that the same interval for transmitting advertisement packets is set on the ports used to connected both devices; otherwise DLDP will not operate properly.*

Resetting DLDP Status

*Only after the ports are DLDP down due to the detection of unidirectional links can you use the **dldp reset** command to reset the DLDP status of these ports to retrieve DLDP probes.*

Table 151 Reset DLDP status

Operation			Command	Description
Reset the status of DLDP	Enter system view		**system-view**	-
	Reset the status of DLDP globally		**dldp reset**	Optional
	Reset the status of DLDP on a port	Enter Ethernet port view	**interface** *interface-type interface-number*	-
		Reset the status of DLDP on 100 M Ethernet ports	**dldp reset**	Optional
		Reset the status of DLDP on Gigabit Ethernet ports	**dldp reset**	

CAUTION:

- *This command only applies to the ports in DLDP down status.*
- *If a port is DLDP down, it can return to the up state automatically. You do not need to reset DLDP on the port.*

Precautions During DLDP Configuration

- DLDP does not work on a port where you configure duplex and rate forcibly, such as 10 GE port.
- DLDP works only when the link is up.
- To insure that DLDP neighbors can be established properly and unidirectional links can be detected, you must make sure: DLDP is enabled on both ends, and the interval of sending DLDP advertisement packets, authentication mode and password are consistent on both ends.
- You can adjust the interval of sending DLDP advertisement packets (which is 5 seconds by default and in the range of 1 seconds to 100 seconds) in different network circumstances, so that DLDP can respond rapidly to link failure. The interval must be shorter than one-third of the STP convergence time, which is generally 30 seconds. If too long an interval is set, an STP loop may occur before DLDP shut down unidirectional links. On the contrary, if too short an interval is set, network traffic increases, and port bandwidth is reduced.
- DLDP is also applicable to STP Discarding ports. Ports discarded by STP can set up normal DLDP neighbors and detect unidirectional links.
- DLDP does not process any LACP event, and treats each link in the aggregation group as independent.
- The mandatory duplex mode must be enabled on both ends of the DLDP link. In this way, unidirectional links will be reported and the ports can be shut down as required; if the auto-negotiation duplex mode is configured on both ends, unidirectional links will not be reported and ports will not be shut down, while only the state of DLDP neighbors changes.
- If DLDP is enabled after unidirectional links appear, DLDP cannot detect unidirectional links.
- DLDP cannot be used together with similar protocols of other companies, that is, you cannot enable DLDP on one end and enable one of the similar protocols of other companies.

For XGbus products, pay attention to the following points:

- When interface modules are hot swapped, if the plugged interface module is of the same type as the pulled interface module, DLDP restores automatically.
- When active/standby switchover is performed on an Fabric, the standby Fabric detects unidirectional links instead of the Fabric. DLDP parameters remain the same and unidirectional links are detected again on each port.

DLDP Network Example

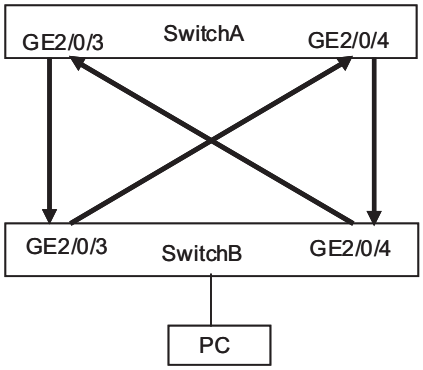
Network requirements

As shown in Figure 57:

- Switch A and Switch B are connected through two pairs of fibers. Both of them support DLDP;
- Suppose the fibers between Switch A and Switch B are cross-connected. DLDP disconnects the unidirectional links after detecting them;
- When the network administrator connects the fiber correctly, the ports taken down by DLDP are restored.

Network diagram

Figure 57 Fiber cross-connection



Configuration procedure

1 Configure Switch A

Configure the ports to work in mandatory full duplex mode at the speed of 1000 Mbps.

```
<SW7750A> system-view
[SW7750A] interface gigabitethernet 2/0/3
[SW7750A-GigabitEthernet2/0/3] duplex full
[SW7750A-GigabitEthernet2/0/3] speed 1000
[SW7750A-GigabitEthernet2/0/3] quit
[SW7750A] interface gigabitethernet 2/0/4
[SW7750A-GigabitEthernet2/0/4] duplex full
[SW7750A-GigabitEthernet2/0/4] speed 1000
[SW7750A-GigabitEthernet2/0/4] quit
```

Enable DLDP globally

```
[SW7750A] dldp enable
```

Set the interval of sending DLDP packets to 15 seconds

```
[SW7750A] dldp interval 15
```

Configure DLDP to work in enhanced mode

```
[SW7750A] dldp work-mode enhance
```

Set the DLDP handling mode to auto after unidirectional links are detected

```
[SW7750A] dldp unidirectional-shutdown auto
```

Display the DLDP status

```
[SW7750A] display dldp
```



If the fibers are correctly connected between the two switches, the system displays the connections with the neighbor as bidirectional links.

When the fibers are not correctly connected:

- *When the fibers are cross-connected, both ends are unidirectional links and the two ends are displayed as in Disable status;*
- *When one end is correctly connected and the other end is not connected, one end is in Advertisement status and the other is in Inactive status.*

Restore the ports taken down by DLDP

```
[SW7750A] dldp reset
```

2 Configure Switch B

The configuration of Switch B is the same to that of Switch A.



Suppose the port works in the mandatory full duplex mode and the connection at both ends of the link is normal. After DLDP is enabled, if the optical fiber in one end is not connected, DLDP will report that the link is a unidirectional link.

28 MAC Address Table Management

This chapter describes the management of static and dynamic MAC address entries. For information on the management of multicast MAC address entries, refer to "Multicast Overview" on page 413.

Overview

Introduction to MAC Address Learning

An Ethernet switch maintains a MAC address table to forward packets quickly. A MAC address table is a port-based Layer 2 address table. It is the base for Ethernet switch to perform Layer 2 packet forwarding. Each entry in a MAC address table contains the following fields:

- Destination MAC address
- ID of the VLAN which a port belongs to.
- Forwarding port number.

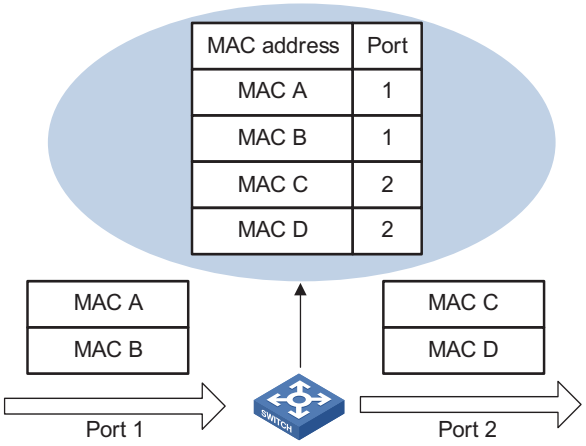
Upon receiving a packet, a switch queries its MAC address table for the forwarding port number according to the destination MAC address carried in the packet and then forwards the packet through the port.

The dynamic address entries (not configured manually) in the MAC address table are learned by the Ethernet switch. When an Ethernet switch learns a MAC address, the following occurs:

When a switch receives a packet from one of its ports (referred to as Port 1), the switch extracts the source MAC address (referred to as MAC-SOURCE) of the packet and considers that the packets destined for MAC-SOURCE can be forwarded through Port 1.

- If the MAC address table already contains MAC-SOURCE, the switch updates the corresponding MAC address entry.
- If MAC-SOURCE does not exist in the MAC address table, the switch adds MAC-SOURCE and Port 1 as a new MAC address entry to the MAC address table.

Figure 58 Packets forwarded by using a MAC address table.



After learning the source address of the packet, the switch searches the MAC address table for the destination MAC address of the received packet:

- If it finds a match, it directly forwards the packet.
- If it finds no match, it forwards the packet to all ports, except the receiving port, within the VLAN to which the receiving port belongs. Normally, this is referred to as broadcasting the packet.

After broadcasting the packet, the switch will do one of the following based on whether it receives a response packet:

- If the network device returns a packet to the switch, this indicates the packet has been sent to the destination device. The MAC address of the device is carried in the packet. The switch adds the new MAC address to the MAC address table through address learning. After that, the switch can directly forward other packets destined for the same network device by using the newly added MAC address entry.
- If the destination device does not respond to the packet, this indicates that the destination device is unreachable or that the destination device receives the packet but gives no response. In this case, the switch still cannot learn the MAC address of the destination device. Therefore, the switch will still broadcast any other packet with this destination MAC address.

To fully utilize a MAC address table, which has a limited capacity, the switch uses an aging mechanism for updating the table. That is, the switch removes the MAC address entries related to a network device if no packet is received from the device within the aging time. Aging time only applies to dynamic MAC address entries.

You can manually configure (add or modify) a static or dynamic MAC address entry based on the actual network environment.

The switch learns only unicast addresses by using the MAC address learning mechanism but directly drops any packet with a broadcast source MAC address.

Entries in a MAC Address Table

Entries in a MAC address table fall into the following two categories according to their characteristics and configuration methods:

- Static MAC address entry: Also known as permanent MAC address entry. This type of MAC address entries are added/removed manually and can not age out by themselves. Using static MAC address entries can reduce broadcast packets remarkably and are suitable for networks where network devices seldom change.
- Dynamic MAC address entry: This type of MAC address entries age out after the configured aging time. They are generated by the MAC address learning mechanism or configured manually.

Table 152 lists the different types of MAC address entries and their characteristics.

Table 152 Characteristics of different types of MAC address entries

MAC address entry	Configuration method	Aging time	Reserved or not at reboot (if the configuration is saved)
Static MAC address entry	Manually configured	Unavailable	Yes
Dynamic MAC address entry	Manually configured or generated by MAC address learning mechanism	Available	No

Configuring MAC Address Table Management

MAC Address Entry Configuration Tasks

Table 153 MAC address entry configuration tasks

Configuration task	Description	Related section
Configure a MAC address entry	Required	"Configuring a MAC Address Entry" on page 227
Set the aging time for MAC addresses	Optional	"Setting the Aging Time for MAC Address Entries" on page 228
Configure the maximum number of MAC addresses that a port can learn	Optional	"Setting the Maximum Number of MAC Addresses a Port Can Learn" on page 228
Disable a port from learning MAC addresses	Optional	"Disabling MAC Address Learning" on page 229
Configure MAC address synchronization between module chips	Optional	"Configuring MAC Address Learning Synchronization Between Module Chips" on page 229
Disable HiGig ports from learning MAC addresses	Optional	"Disabling HiGig Ports from Learning MAC Addresses" on page 229.

Configuring a MAC Address Entry

You can add, modify, or remove one MAC address entry, remove all the MAC address entries (unicast MAC addresses only) concerning a specific port, or remove a specific type of MAC address entries (dynamic or static).

Table 154 Add a MAC address entry

Operation	Command	Description
Enter system view	**system-view**	-
Add a MAC address entry	**mac-address** { **static** | **dynamic** } *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*	Required

CAUTION: *For a MAC address entry to be added, the port specified by the* ***interface*** *keyword must belong to the VLAN specified by the* ***vlan*** *keyword in the command. Otherwise, the entry will not be added.*

Setting the Aging Time for MAC Address Entries

Setting aging time properly helps implement effective MAC address aging. The aging time that is too long or too short results in a large amount of broadcast packets wandering across the network and decreases the performance of the switch.

- If the aging time is too long, excessive invalid MAC address entries maintained by the switch may fill up the MAC address table. This prevents the MAC address table from varying with network changes in time.
- If the aging time is too short, the switch may remove valid MAC address entries. This decreases the forwarding performance of the switch.

Table 155 Set aging time for MAC address entries

Operation	Command	Description
Enter system view	**system-view**	-
Set the aging time of MAC address entries	**mac-address timer** { **aging** *age* | **no-aging** }	Required The default aging time is 300 seconds.

This command is used in system view and applies to all ports. Aging applies to only dynamic MAC addresses that are learnt or configured to age.

Normally, you are recommended to use the default aging time, namely, 300 seconds. The **no-aging** keyword specifies that MAC address entries do not age out.

Setting the Maximum Number of MAC Addresses a Port Can Learn

The MAC address learning mechanism enables an Ethernet switch to acquire the MAC addresses of the network devices on the segment connected to the ports of the switch. The switch directly forwards the packets destined for these MAC addresses. An oversized MAC address table may decrease the forwarding performance of the switch.

By setting the maximum number of MAC addresses that can be learnt from individual ports, you can control the number of the MAC address entries the MAC address table can dynamically maintains. If you have set the maximum number of MAC addresses that a port can learn to *count*, the port stops learning MAC addresses when the number of MAC addresses learned by the port reaches *count*.

Table 156 Set the maximum number of MAC addresses a port can learn

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Set the maximum number of MAC addresses the port can learn	**mac-address max-mac-count** *count*	Required By default, the number of the MAC addresses a port can learn is not limited.

Disabling MAC Address Learning

To gain better control over network security, you can use the following commands to disable the current port from learning MAC addresses.

Table 157 Disable the current port from learning MAC addresses

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Disable the current port from learning MAC addresses	**mac-address mac-learning disable**	Required By default, the port is enabled to learn MAC addresses.

- *Do not use the **mac-address mac-learning disable** command together with related 802.1x commands in Ethernet port view.*
- *Do not use the **mac-address mac-learning disable** command together with the **mac-address max-mac-count** command.*

Configuring MAC Address Learning Synchronization Between Module Chips

If there are multiple chips on a module, each chip can learn only the MAC addresses of the data flow it handles. If a chip receives a packet whose MAC address entry is stored in another chip, it broadcasts the packet.

You can configure MAC address learning synchronization between module chips to synchronize MAC address entries between chips. This reduces broadcasting of unknown packets, lowers switch processing load, and improves network utilization.

Table 158 Configure MAC address learning synchronization between module chips

Operation	Command	Description
Enter system view	**system-view**	-
Enable MAC address learning synchronization between module chips	**mac-address learning synchronization**	Optional By default, MAC address learning synchronization between module chips is disabled.

Disabling HiGig Ports from Learning MAC Addresses

The Switch 7750 learn MAC address entries in one of the following ways:

- Through MAC address learning on the port
- By synchronizing MAC address entries between chips

HiGig ports are special ports on modules for connecting the modules to the backplane. HiGig ports can also learn and synchronize MAC addresses. With such characteristics, HiGig ports may bring about the following issue:

With MAC address learning disabled on a port and MAC address learning synchronization between module chips enabled globally (See "Configuring MAC Address Learning Synchronization Between Module Chips" on page 229), if the packets received on the port are to be forwarded or broadcast through HiGig ports to the ports of other module chips, those chips will learn the MAC address entry whose source MAC address matches the ingress port and synchronize the entry back to the chip of the ingress port through MAC address learning synchronization between module chips. This causes the configuration of disabling MAC address learning on the ingress port to be ineffective.

To address this issue, you can disable HiGig ports from learning MAC addresses.

Table 159 Disable HiGig ports from learning MAC addresses

Operation	Command	Description
Enter system view	**system-view**	-
Disable HiGig ports from learning MAC addresses	**higig-port mac-learning disable** *slot-number*	Optional By default, HiGig ports are enabled to learn MAC addresses.



The above-mentioned command is not available for the following modules: 3C16860, 3C16861, LS81FS24A, 3C16858, 3C16859, LS8M1PT4GB0, LS8M1PT8GB0, LS81PT4GA, and LS81PT8GA.

Setting the processing method for the specific packets

You can use the following commands to configure whether or not the packets with destination MAC address being the bridge MAC address of the switch will be passed to CPU for processing.

Table 160 Set the processing method for the specific packets

Operation	Command	Description
Enter system view	**system-view**	-
Enable the packets with destination MAC address as the bridge MAC address of the switch to be passed to the CPU for processing	**bridgemactocpu enable**	Optional By default, the packets with destination MAC address as the bridge MAC address of the switch are not passed to the CPU for processing.
Disable the packets with destination MAC address as the bridge MAC address of the switch from being passed to the CPU for processing	**bridgemactocpu disable**	Optional

Displaying and Maintaining MAC Address Configuration

To verify your configuration, you can display information about the MAC address table by executing the **display** command in any view.

Table 161 Display and maintain MAC address table configuration

Operation	Command	Description
Display information about the MAC address table	**display mac-address** [*display-option*]	You can use the **display** command in any view.
Display the aging time of the dynamic MAC address entries in the MAC address table	**display mac-address aging-time**	

Configuration Example

Network requirements

- Log in to the switch through the Console port and enable address table configuration.
- Set the aging time of dynamic MAC address entries to 500 seconds.
- Add a static MAC address entry 000f-e235-dc71 for Ethernet2/0/2 port (assuming that the port belongs to VLAN 1)

Configuration procedure

Enter system view.

```
<SW7750> system-view
[SW7750]
```

Add a MAC address, with the VLAN, ports, and states specified.

```
[SW7750] mac-address static 000f-e235-dc71 interface Ethernet 2/0/2 vlan 1
```

Set the aging time of dynamic MAC addresses to 500 seconds.

```
[SW7750] mac-address timer aging 500
```

Display the information about the MAC address entries in system view.

```
[SW7750] display mac-address interface Ethernet 2/0/2
MAC ADDR         VLAN ID   STATE             PORT INDEX             AGING TIME(s)
000f-e235-dc71     1       Config static    Ethernet2/0/2          NOAGED
000f-e200-5503     1       Learned          Ethernet2/0/2          445
000f-e200-5548     1       Learned          Ethernet2/0/2          282
---  3 mac address(es) found on port Ethernet2/0/2 ---
```

29 CENTRALIZED MAC ADDRESS AUTHENTICATION CONFIGURATION

Currently, 3C16860, 3C16861, LS81FS24A, 3C16859, and 3C16858 I/O Modules of 3Com Switch 7750 Ethernet switches do not support the centralized MAC address authentication.

Centralized MAC Address Authentication Overview

Centralized MAC address authentication is port- and MAC address-based authentication used to control user permissions to access a network. Centralized MAC address authentication can be performed without client-side software. With this type of authentication employed, a switch authenticates a user upon detecting the MAC address of the user for the first time.

Centralized MAC address authentication can be implemented in the following two modes:

- MAC address mode, where user MAC serves as both the user name and the password.
- Fixed mode, where user names and passwords are configured on a switch in advance.

As for Switch 7750 Ethernet switches, authentication can be performed locally or through a RADIUS server.

1. When a RADIUS server is used for authentication, the switch serves as a RADIUS client. Authentication is carried out through the cooperation of switches and the RADIUS server.
   - In MAC address mode, a switch sends user MAC addresses detected to the RADIUS server as both user names and passwords. The rest handling procedures are the same as that of the common RADIUS authentication.
   - In fixed mode, a switch sends the user name and password previously configured for the user to be authenticated to the RADIUS server and replaces the calling-station-id field of the RADIUS packet with the MAC address of the user. The rest handling procedures are the same as that of the common RADIUS authentication.
   - A user can access a network upon passing the authentication performed by the RADIUS server.
2. When authentications are performed locally, users are authenticated by switches. In this case,
   - For fixed mode, configure the local user names and passwords as those for fixed mode.
   - The service type of a local user needs to be configured as lan-access.

Centralized MAC Address Authentication Configuration

The following are centralized MAC address authentication configuration tasks:

- "Enabling Centralized MAC Address Authentication Globally" on page 234
- "Enabling Centralized MAC Address Authentication for a Port" on page 234
- "Configuring Centralized MAC Address Authentication Mode" on page 235
- "Configuring the ISP Domain for MAC Address Authentication Users" on page 235
- "Configuring the Timers Used in Centralized MAC Address Authentication" on page 236
- "Configuring Centralized MAC Address Re-Authentication" on page 236



CAUTION: *The configuration of the maximum number of learned MAC addresses (refer to the* ***mac-address max-mac-count*** *command) is unavailable for the ports with centralized MAC address authentication enabled. Similarly, the centralized MAC address authentication is unavailable for the ports with the maximum number of learned MAC addresses configured.*

- *If a port is enabled with the centralized MAC address authentication, you cannot configure the maximum number of MAC addresses that the port can learn. And, if you have configured the maximum number of MAC addresses that the port can learn, you are not allowed to enable the centralized MAC address authentication function on the port.*
- *If a port is already enabled with the 802.1x function, and the access control mode of the port is not configured as* ***macbased****, you are not allowed to enable the centralized MAC address authentication function on the port.*
- *If a port is already enabled with the centralized MAC address authentication function, you cannot add the port to a link aggregation group. And, if the port is already in a aggregation group, you are not allowed to enable the centralized MAC address authentication function on the port.*
- *If a port is enabled with the centralized MAC address authentication function, you cannot configure the port as a reflector port, and vice versa.*
- *You cannot enable both the port security feature and the centralized MAC address authentication function on a port.*

Enabling Centralized MAC Address Authentication Globally

Table 162 Enable centralized MAC address authentication globally

Operation	Command	Description
Enter system view	**system-view**	-
Enable centralized MAC address authentication globally	**mac-authentication**	Required By default, centralized MAC address authentication is globally disabled.

Enabling Centralized MAC Address Authentication for a Port

You can enable centralized MAC address authentication for a port in system view or in Ethernet port view.

Table 163 Enable centralized MAC address authentication for a port in system view

Operation	Command	Description
Enter system view	**system-view**	-
Enable centralized MAC address authentication for specified ports	**mac-authentication interface** *interface-list*	Required By default, centralized MAC address authentication is disabled on a port.

Table 164 Enable centralized MAC address authentication for a port in Ethernet port view

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Enable centralized MAC address authentication for the current port	**mac-authentication**	Required By default, centralized MAC address authentication is disabled on a port.

Centralized MAC address authentication for a port can be configured but does not take effect before global centralized MAC address authentication is enabled. After global centralized MAC address authentication is enabled, ports enabled with the centralized MAC address authentication will perform the authentication immediately.

Configuring Centralized MAC Address Authentication Mode

Table 165 Configure centralized MAC address authentication mode

Operation	Command	Description
Enter system view	**system-view**	-
Configure centralized MAC address authentication mode as MAC address mode	**mac-authentication authmode usernameasmacaddress** [**usernameformat** { **with-hyphen** | **without-hyphen** }]	Optional By default, the MAC address mode is adopted.
Configure centralized MAC address authentication mode as fixed mode	**mac-authentication authmode usernamefixed**	
Set a user name for fixed mode	**mac-authentication authusername** *username*	Optional By default, the user name is mac and no password is configured.
Set the password for fixed mode	**mac-authentication authpassword** *password*	

Configuring the ISP Domain for MAC Address Authentication Users

Table 166 lists the operations to configure the ISP domain for centralized MAC address authentication users.

Table 166 Configure the ISP domain for centralized MAC address authentication users

Operation	Command	Description
Enter system view	**system-view**	-

Table 166 Configure the ISP domain for centralized MAC address authentication users

Operation	Command	Description
Configure the ISP domain for MAC address authentication users	**mac-authentication domain** *isp-name*	Required By default, the "default domain" is used as the ISP domain.

Configuring the Timers Used in Centralized MAC Address Authentication

The following timers are used in centralized MAC address authentication:

- Offline detect timer, which sets the time interval for a switch to test whether a user goes offline. Upon detecting a user is offline, a switch notifies the RADIUS server of the user to trigger the RADIUS server to stop the accounting on the user.
- Quiet timer, which sets the quiet period for a switch. After a user fails to pass the authentication performed by a switch, the switch quiets for a specific period (the quiet period) before it authenticates users again.
- Server timeout timer. During authentication, the switch prohibits the user from accessing the network through the corresponding port if the connection between the switch and RADIUS server times out. In this case, the user can have it authenticated through another port of the switch.
- Reauth-period timer. After a user pass the MAC address authentication, the switch will periodically request the server for re-authentication. The period is determined by the Reauth-period server.

Table 167 lists the operations to configure the timers used in centralized MAC address authentication.

Table 167 Configure the timers used in centralized MAC address authentication

Operation	Command	Description
Enter system view	**system-view**	-
Configure a timer used in centralized MAC address authentication	**mac-authentication timer** { **offline-detect** *offline-detect-value* | **quiet** *quiet-value* | **server-timeout** *server-timeout-value* | **reauth-period** *reauth-period-value* }	Optional The default settings of the timers used in centralized MAC address authentication are as follows: ■ Offline detect timer: 300 seconds ■ Quiet timer: 60 seconds ■ Server timeout timer: 100 seconds ■ Reauth-period timer: 1800 seconds

Configuring Centralized MAC Address Re-Authentication

Re-authentication function enables a switch to re-authenticate a user's identity or change his authentication information when necessary if the user adopts the MAC address authentication to access the network.

Table 168 Configure the centralized MAC address re-authentication function

Operation	Command	Description
Enter system view	**system-view**	-
Enable the MAC address regular re-authentication function	**mac-authentication re-authenticate enable**	Optional By default, the MAC address regular re-authentication function is disabled.
Configure to re-authenticate a specified MAC address	**mac-authentication re-authenticate mac-address** *mac-address*	Optional



- *If the MAC address regular re-authentication function is enabled, when the Reauth-period times out, the device initiates a re-authentication.*
- *When you configure to re-authenticate a user with the specified MAC address, each MAC address re-authentication configuration on the user will trigger a re-authentication. If re-authentication succeeds, the user will be authorized; otherwise, the user will be made offline.*
- *When you configure to re-authenticate a specified MAC address, if the MAC address has failed the MAC address authentication, the re-authentication operation will be ignored.*

Displaying and Debugging Centralized MAC Address Authentication

After the above configuration, you can execute the **display** command in any view to display system running of centralized MAC address authentication configuration, and to verify the effect of the configuration. You can execute the **reset** command in user view to clear the statistics of centralized MAC address authentication.

Table 169 Display and debug centralized MAC address authentication

Operation	Command	Description
Display global or port information about centralized MAC address authentication	**display mac-authentication** [**interface** *interface-list*]	This command can be executed in any view.
Clear the statistics of global or port centralized MAC address authentication	**reset mac-authentication statistics** [**interface** *interface-list*]	This command is executed in user view

Centralized MAC Address Authentication Configuration Example



Centralized MAC address authentication configuration is similar to that of 802.1x. In this example, the differences between the two lie in

- *Centralized MAC address authentication needs to be enabled both globally and for a port.*
- *In MAC address mode, MAC address of locally authenticated user is used as both user name and password.*

- *In MAC address mode, MAC address of user authenticated by RADIUS server need to be configured as both user name and password on the RADIUS server.*

Network requirement

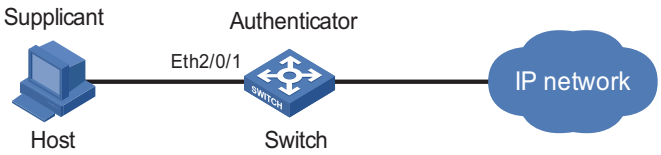
As shown in the following figure, a user workstation (Supplicant) is connected with Ethernet 2/0/1 of the Ethernet device (Authenticator).

The device administrator intends to perform

- The device administrator intends to control users to access the internet by performing MAC address authentication on all ports of the device.
- The device tests whether the user is offline every 180 seconds. And when the user authentication fails, the device waits for 30 seconds before it authenticates the user again.
- All users belong to domain aabbcc.net, adopting the local authentication mode. The user name and password are both 000fe2010101.

Network diagram

Figure 59 Enable to perform the MAC address authentication locally for access users



Configuration Procedure

Add a local access user.

```
<SW7750> system-view
[SW7750] local-user 000fe2010101
[SW7750-luser-000fe2010101] password simple 000fe2010101
[SW7750-luser-000fe2010101] service-type lan-access
[SW7750-luser-000fe2010101] quit
```

Configure the ISP domain, and use the local authentication mode.

```
[SW7750] domain aabbcc.net
[SW7750-isp-aabbcc.net] authentication lan-access local
[SW7750-isp-aabbcc.net] quit
```

Enable the MAC address authentication function globally.

```
[SW7750] mac-authentication
```

Enable MAC address authentication for the specified port Ethernet 2/0/1.

```
[SW7750] mac-authentication interface Ethernet 2/0/1
```

Configure MAC address authentication users to use the ISP domain aabbcc.net.

```
[SW7750] mac-authentication domain aabbcc.net
```

Configure MAC address authentication timers.

```
[SW7750] mac-authentication timer offline-detect 180
[SW7750] mac-authentication timer quiet 30
```

For domain-related configuration, refer to the "802.1x Configuration Example" on page 404.

30 MSTP CONFIGURATION

MSTP Overview

Spanning tree protocol (STP) cannot enable Ethernet ports to transit their states rapidly. It costs two times of the forward delay for a port to transit to the forwarding state even if the port is on a point-to-point link or the port is an edge port. This slows down the spanning tree convergence of STP.

Rapid spanning tree protocol (RSTP) enables the spanning tree to converge rapidly, but it suffers from the same drawback as that of STP: all bridges in a LAN share one spanning tree; packets of all VLANs are forwarded along the same spanning tree, and therefore redundant links cannot be blocked by VLANs.

As well as the above two protocols, multiple spanning tree protocol (MSTP) can disbranch a ring network to form a tree-topological ring-free network to prevent packets from being duplicated and forwarded endlessly in the ring network. Besides this, MSTP can also provide multiple redundant paths for packet forwarding and balances the forwarding loads of different VLANs.

MSTP is compatible with both STP and RSTP. It overcomes the drawback of STP and RSTP. It not only enables spanning trees to converge rapidly, but also enables packets of different VLANs to be forwarded along their respective paths to provide a better load-balancing mechanism with redundant links.

MSTP Protocol Data Unit

Bridge protocol data unit (BPDU) is the protocol data unit (PDU) that STP and RSTP use.

The switches in a network transfer BPDUs between each other to determine the topology of the network. BPDUs carry the information that is needed for switches to figure out the spanning tree.

BPDUs used in STP fall into the following two categories:

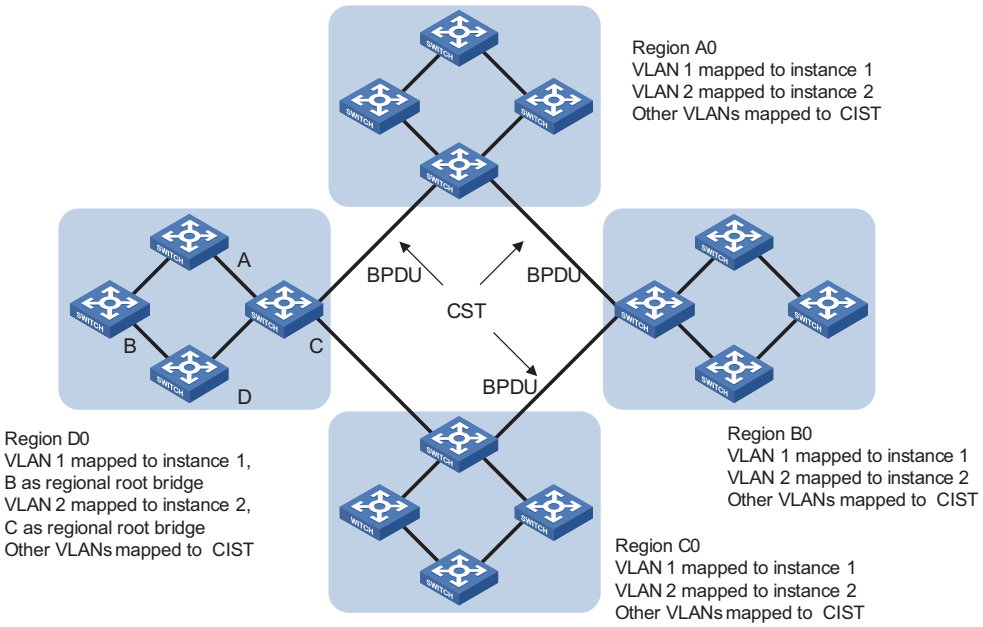
- Configuration BPDUs: BPDUs of this type are used to maintain the spanning tree topology.
- Topology change notification BPDU (TCN BPDN): BPDUs of this type are used to notify the switches of network changes.

Similar to STP and RSTP, MSTP uses BPDUs to figure out spanning trees too. Besides, the BPDUs of MSTP carry MSTP configuration information of the switches.

Basic MSTP Terminologies

Figure 60 illustrates basic MSTP terms (assuming that MSTP is enabled on each switch in this figure).

Figure 60 Basic MSTP terminologies



MST region

An MST region (multiple spanning tree region) comprises multiple physically-interconnected MSTP-enabled switches and the corresponding network segments connected to these switches. These switches have the same region name, the same VLAN-to-spanning-tree mapping configuration and the same MSTP revision level.

A switched network can contain multiple MST regions. You can group multiple switches into one MST region by using the corresponding MSTP configuration commands. For example, all switches in region A0 shown in Figure 60 have the same MST region configuration: the same region name, the same VLAN-to-spanning-tree mappings (that is, VLAN 1 is mapped to spanning tree instance 1, VLAN 2 is mapped to spanning tree instance 2, and other VLANs are mapped to CIST), the same MSTP revision level (not shown in Figure 60).

MSTI

A multiple spanning tree instance (MSTI) refers to a spanning tree in a MST region.

Multiple spanning trees can be established in one MST region. These spanning trees are independent of each other. For example, each region in Figure 60 contains multiple spanning trees known as MSTIs (multiple spanning tree instances). Each of these spanning trees corresponds to a VLAN.

VLAN mapping table

A VLAN mapping table is a property of an MST region. It contains information about how VLANs are mapped to MSTIs. For example, in Figure 60, the information contained in the VLAN mapping table of region A0 is: VLAN 1 is mapped to MSTI 1; VLAN 2 is mapped to MSTI 2; and other VLANs are mapped to CIST. In an MST region, load balancing is achieved by the VLAN mapping table.

IST

An internal spanning tree (IST) is a spanning tree in an MST region.

ISTs together with the common spanning tree (CST) form the common and internal spanning tree (CIST) of the entire switched network. An IST is a special MSTI; it belongs to an MST region and is a branch of CIST. In Figure 60, each MST region has an IST, which is a branch of the CIST.

CST

A CST is the spanning tree in a switched network that connects all MST regions in the network. If you regard each MST region in the network as a switch, then the CST is the spanning tree generated by STP or RSTP running on the "switches". In Figure 60, the lines in red depict the CST.

CIST

A CIST is the spanning tree in a switched network that connects all switches in the network. It comprises the ISTs and the CST. In Figure 60, the ISTs in the MST regions and the CST connecting the MST regions form the CIST.

Region root

A region root is the root of the IST or an MSTI in a MST region. Different spanning trees in an MST region may have different topologies and thus have different region roots. In region D0 shown in Figure 60, the region root of MSTI 1 is switch B, and the region root of MSTI 2 is switch C.

Common root bridge

The common root bridge is the root of the CIST. The common root bridge of the network shown in Figure 60 is a switch in region A0.

Port roles

In MSTP, the following port roles exist: root port, designated port, master port, region edge port, alternate port, and backup port.

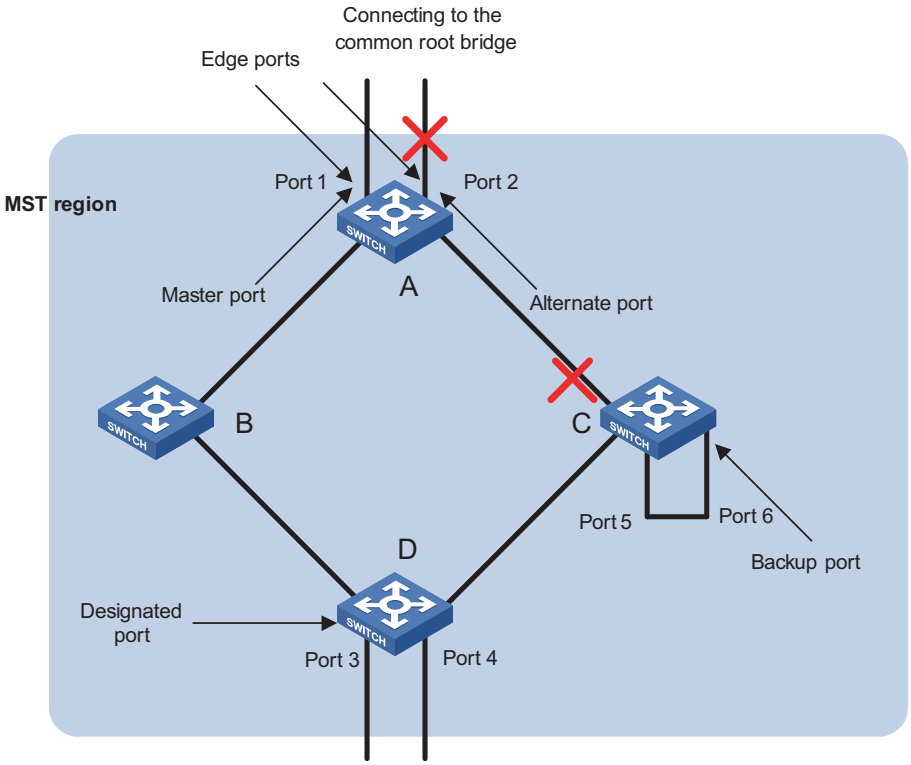
- A root port is used to forward packets to the root.
- A designated port is used to forward packets to a downstream network segment or switch.
- A master port connects a MST region to the common root. The path from the master port to the common root is the shortest path between the MST region and the common root.
- A region edge port is located on the edge of an MST region and is used to connect the MST region to another MST region, an STP-enabled region or an RSTP-enabled region
- An alternate port is a backup port of a master port. It becomes the master port if the existing master port is blocked.
- A loop occurs when two ports of a switch are connected to each other. In this case, the switch blocks one of the two ports. The blocked port is a backup port.

In Figure 61, switch A, B, C, and D form an MST region. Port 1 and port 2 on switch A connect upstream to the common root. Port 5 and port 6 on switch C

form a loop. Port 3 and port 4 on switch D connect downstream to other MST regions. This figure shows the roles these ports play.

- *A port can play different roles in different MSTIs.*
- *The role a region edge port plays is consistent with the role it plays in the CIST. For example, port 1 on switch A in Figure 61 is a region edge port, and it is a master port in the CIST. So it is a master port in all MSTIs in the region.*

Figure 61 Port roles



Port states

Ports can be in the following three states:

- Forwarding state: Ports in this state can forward user packets and receive/send BPDU packets.
- Learning state: Ports in this state can receive/send BPDU packets.
- Discarding state: Ports in this state can only receive BPDU packets.

Table 170 lists possible combinations of port states and port roles.

Table 170 Combinations of port states and port roles

Port State \ Port Role	Root/ port/Master port	Designated port	Region edge port	Alternate port	Backup port
Forwarding	√	√	√	-	-
Learning	√	√	√	-	-
Discarding	√	√	√	√	√

Implementation of MSTP

MSTP divides a network into multiple MST regions at Layer 2. The CST is generated between these MST regions, and multiple spanning trees (or, MSTIs) can be generated in each MST region. As well as RSTP, MSTP uses configuration BPDUs to generate spanning trees. The only difference is that the configuration BPDUs for MSTP carry the MSTP configuration information on the switches.

Generating the CIST

Through configuration BPDU comparing, the switch that is of the highest priority in the network is chosen as the root of the CIST. In each MST region, an IST is figured out by MSTP. At the same time, MSTP regards each MST region as a switch to figure out the CST of the network. The CST, together with the ISTs, forms the CIST of the network.

Generating an MSTI

In an MST region, different MSTIs are generated for different VLANs depending on the VLAN-to-spanning-tree mappings. Each spanning tree is figured out independently, in the same way as STP/RSTP.

Implementation of STP algorithm

In the beginning, each switch regards itself as the root, and generates a configuration BPDU for each port on it as a root, with the root path cost being 0, the ID of the designated bridge being that of the switch, and the designated port being itself.

1 Each switch sends out its configuration BPDUs and operates in the following way when receiving a configuration BPDU on one of its ports from another switch:

- If the priority of the configuration BPDU is lower than that of the configuration BPDU of the port itself, the switch discards the BPDU and does not change the configuration BPDU of the port.
- If the priority of the configuration BPDU is higher than that of the configuration BPDU of the port itself, the switch replaces the configuration BPDU of the port with the received one and compares it with those of other ports on the switch to obtain the one with the highest priority.

2 Configuration BPDUs are compared as follows:

- The smaller the root ID of the configuration BPDU is, the higher the priority of the configuration BPDU is.
- For configuration BPDUs with the same root IDs, the comparison is based on the path costs. Suppose S is the sum of the root path cost and the corresponding path cost of the port. The less the S value is, the higher the priority of the configuration BPDU is.
- For configuration BPDUs with both the same root ID and the same root path cost, the designated bridge ID, designated port ID, the ID of the receiving port are compared in turn.

3 A spanning tree is figured out as follows:

- Determining the root bridge

The root bridge is selected by configuration BPDU comparing. The switch with the smallest root ID is chosen as the root bridge.

- Determining the root port

For each switch in a network, the port through which the configuration BPDU with the highest priority is received is chosen as the root port of the switch.

- Determining the designated port

First, the switch generates a designated port configuration BPDU for each of its port using the root port configuration BPDU and the root port path cost, with the root ID being replaced with that of the root port configuration BPDU, root path cost being replaced with the sum of the path cost of the root port configuration BPDU and the path cost of the root port, the ID of the designated bridge being replaced with that of the switch, and the ID of the designated port being replaced with that of the port.

The switch then compares the resulting configuration BPDU with the original configuration BPDU received from the corresponding port on another switch. If the latter takes precedence over the former, the switch blocks the local port and remains the port's configuration BPDU unchanged, so that the port can only receive configuration messages and cannot forward packets. Otherwise, the switch sets the local port to the designated port, replaces the original configuration BPDU of the port with the resulting one and releases it regularly.

MSTP Implementation on Switches

MSTP is compatible with both STP and RSTP. That is, switches with MSTP employed can recognize the protocol packets of STP and RSTP and use them to generate spanning trees. In addition to the basic MSTP functions, 3Com series switches also provide the following other functions for the convenience of users to manage their switches.

- Root bridge retaining
- Root bridge backup
- Root protection
- BPDU protection
- Loop guard

Root Bridge Configuration

Table 171 lists MSTP-related configurations about root bridges.

Table 171 Root bridge configuration

Operation	Remarks	Related section
MSTP configuration	Required To prevent network topology jitter caused by other related configurations, you are recommended to enable MSTP after other related configurations are performed.	"MSTP Configuration" on page 258
MST region configuration	Required	"MST Region Configuration" on page 247
Root bridge/secondary root bridge configuration	Required	"Root Bridge/Secondary Root Bridge Configuration" on page 249

Table 171 Root bridge configuration

Operation	Remarks	Related section
Bridge priority configuration	Optional The priority of a switch cannot be changed after the switch is specified as the root bridge or a secondary root bridge.	"Bridge Priority Configuration" on page 250
MSTP operation mode configuration	Optional	"MSTP Operation Mode Configuration" on page 250
Maximum hops of MST region configuration	Optional	"MST Region Maximum Hops Configuration" on page 251
Network diameter configuration	Optional The default is recommended.	"Network Diameter Configuration" on page 252
MSTP time-related configuration	Optional The defaults are recommended.	"MSTP Time-related Configuration" on page 252
Timeout time factor configuration	Optional	"Timeout Time Factor Configuration" on page 254
Maximum transmitting speed configuration	Optional The default is recommended.	"Maximum Transmitting Speed Configuration" on page 254
Edge port configuration	Optional	"Edge Port Configuration" on page 255
Point-to-point link related configuration	Optional	"Point-to-point Link-Related Configuration" on page 256



In a network that contains switches with both GVRP and MSTP employed, GVRP packets are forwarded along the CIST. If you want to broadcast packets of a specific VLAN through GVRP, be sure to map the VLAN to the CIST when configuring the MSTP VLAN mapping table (The CIST of a network is the spanning tree instance numbered 0.)

Prerequisites The status of the switches in the spanning trees are determined. That is, the status (root, branch, or leaf) of each switch in each spanning tree instance is determined.

MST Region Configuration

Configuration procedure

Table 172 Configure an MST region

Operation	Command	Description
Enter system view	**system-view**	-
Enter MST region view	**stp region-configuration**	-
Configure a name for the MST region	**region-name name**	Required The default MST region name of a switch is its MAC address.
Configure the VALN mapping table for the MST region	**instance** *instance-id* **vlan** *vlan-list*	Required Both commands can be used to configure VLAN mapping tables. By default, all VLANs in an MST region are mapped to spanning tree instance 0.
	vlan-mapping modulo *modulo*	

Table 172 Configure an MST region

Operation	Command	Description
Configure the MSTP revision level for the MST region	**revision-level** *level*	Required The default revision level of an MST region is level 0.
Activate the configuration of the MST region manually	**active region-configuration**	Required
Display the configuration of the current MST region	**check region-configuration**	Optional
Display the currently valid configuration of the MST region	**Display stp region-configuration**	You can execute this command in any view.

Configuring MST region-related parameters (especially the VLAN mapping table) results in spanning trees being regenerated. To reduce network topology jitter caused by the configuration, MSTP does not regenerate spanning trees immediately after the configuration; it does this only after you perform one of the following operations, and then the configuration can really takes effect:

- Activating the new MST region-related settings by using the **active region-configuration** command
- Enabling MSTP by using the **stp enable** command



Switches belong to the same MST region only when they have the same MST region name, VLAN mapping table, and MSTP revision level.

Configuration example

Configure an MST region, with the name being "info", the MSTP revision level being level 1, VLAN 2 through VLAN 10 being mapped to spanning tree instance 1, and VLAN 20 through VLAN 30 being mapped to spanning tree 2.

```
<SW7750> system-view
[SW7750] stp region-configuration
[SW7750-mst-region] region-name info
[SW7750-mst-region] instance 1 vlan 2 to 10
[SW7750-mst-region] instance 2 vlan 20 to 30
[SW7750-mst-region] revision-level 1
[SW7750-mst-region] active region-configuration
```

Verify the above configuration.

```
[SW7750-mst-region] check region-configuration
Admin configuration
   Format selector    :0
   Region name        :info
   Revision level     :1

   Instance   Vlans Mapped
      0       11 to 19, 31 to 4094
      1       1 to 10
      2       20 to 30
```

Root Bridge/Secondary Root Bridge Configuration

MSTP can automatically choose a switch as a root bridge. You can also manually specify the current switch as a root bridge by using the corresponding commands.

Root bridge configuration

Table 173 Specify the current switch as the root bridge of a specified spanning tree

Operation	Command	Description
Enter system view	**system-view**	-
Specify the current switch as the root bridge of a specified spanning tree	**stp** [**instance** *instance-id*] **root primary** [**bridge-diameter** *bridgenumber* [**hello-time** *centi-seconds*]]	Required

Secondary root bridge configuration

Table 174 Specify the current switch as the secondary root bridge of a specified spanning tree

Operation	Command	Description
Enter system view	**system-view**	-
Specify the current switch as the secondary root bridge of a specified spanning tree	**stp** [**instance** *instance-id*] **root secondary** [**bridge-diameter** *bridgenumber* [**hello-time** *centi-seconds*]]	Required

Using the **stp root primary/stp root secondary** command, you can specify a switch as the root bridge or the secondary root bridge of the spanning tree instance identified by the *instance-id* argument. If the value of the *instance-id* argument is set to 0, the **stp root primary/stp root secondary** command specify the current switch as the root bridge or the secondary root bridge of the CIST.

A switch can play different roles in different spanning tree instances. That is, it can be the root bridges in a spanning tree instance and be a secondary root bridge in another spanning tree instance at the same time. But in one spanning tree instance, a switch cannot be the root bridge and the secondary root bridge simultaneously.

When the root bridge fails or is turned off, the secondary root bridge becomes the root bridge if no new root bridge is configured. If you configure multiple secondary root bridges for a spanning tree instance, the one with the least MAC address replaces the root bridge when the latter fails.

You can specify the network diameter and the Hello time parameters while configuring a root bridge/secondary root bridge. Refer to "Network Diameter Configuration" on page 252 and "MSTP Time-related Configuration" on page 252 for information about the network diameter parameter and the Hello time parameter.



- *You can configure a switch as the root bridges of multiple spanning tree instances. But you cannot configure two or more root bridges for one spanning tree instance. So, do not configure root bridges for the same spanning tree instance on two or more switches using the stp root primary command.*
- *You can configure multiple secondary root bridges for one spanning tree instance. That is, you can configure secondary root bridges for the same*

spanning tree instance on two or more switches using the stp root secondary command.

- *You can also configure the current switch as the root bridge by setting the priority of the switch to 0. Note that once a switch is configured as the root bridge or a secondary root bridge, its priority cannot be modified.*

Configuration example

Configure the current switch as the root bridge of spanning tree instance 1 and a secondary root bridge of spanning tree instance 2.

```
<SW7750> system-view
[SW7750] stp instance 1 root primary
[SW7750] stp instance 2 root secondary
```

Bridge Priority Configuration

Root bridges are selected by the bridge priorities of switches. You can make a specific switch being selected as a root bridge by set a higher bridge priority for the switch (Note that a smaller bridge priority value indicates a higher bridge priority.) A MSTP-enabled switch can have different bridge priorities in different spanning tree instances.

Configuration procedure

Table 175 Assign a bridge priority to a switch

Operation	Command	Description
Enter system view	**system-view**	-
Set a bridge priority for the current switch	**stp** [**instance** *instance-id*] **priority** *priority*	Required The default bridge priority of a switch is 32,768.

CAUTION:

- *Once you specify a switch as the root bridge or a secondary root bridge by using the stp root primary or stp root secondary command, the bridge priority of the switch is not configurable.*
- *During the selection of the root bridge, if multiple switches have the same bridge priority, the one with the least MAC address becomes the root bridge candidate.*

Configuration example

Set the bridge priority of the current switch to 4,096 in spanning tree instance 1.

```
<SW7750> system-view
[SW7750] stp instance 1 priority 4096
```

MSTP Operation Mode Configuration

A MSTP-enabled switch can operate in one of the following operation modes:

- STP-compatible mode: In this mode, the protocol packets sent out of the ports of the switch are STP packets. If the switched network contains STP-enabled switches, you can configure the current MSTP-enabled switch to operate in this mode by using the **stp mode stp** command.
- RSTP-compatible mode: In this mode, the protocol packets sent out of the ports of the switch are RSTP packets. If the switched network contains

RSTP-enabled switches, you can configure the current MSTP-enabled switch to operate in this mode by using the **stp mode rstp** command.

- MSTP mode: In this mode, the protocol packets sent out of the ports of the switch are MSTP packets, or STP packets if the ports have STP-enabled switches connected. But multiple spanning tree function is only enabled for MSTP packets.

Configuration procedure

Table 176 Configure MSTP operation mode

Operation	Command	Description
Enter system view	**system-view**	-
Configure the MSTP operation mode for the switch	**stp mode** { **stp** | **rstp** | **mstp** }	Required A MSTP-enabled switch operates in the MSTP mode by default.

Configuration example

Configure the current switch to operate in the STP-compatible mode.

```
<SW7750> system-view
[SW7750] stp mode stp
```

MST Region Maximum Hops Configuration

The maximum hops values configured on the region roots in an MST region limit the size of the MST region.

A configuration BPDU contains a field that maintains the remaining hops of the configuration BPDU. And a switch discards the configuration BPDUs whose remaining hops are 0. After a configuration BPDU reaches a root bridge of a spanning tree in a MST region, the value of the remaining hops field in the configuration BPDU is decreased by 1 every time the configuration BPDU passes a switch. Such a mechanism disables the switches that are beyond the maximum hops from participating in spanning tree generation, and thus limits the size of an MST region.

With such a mechanism, the maximum hops configured on the switch operating as the root bridge of the IST or an MSTI in a MST region becomes the network diameter of the spanning tree, which limits the size of the spanning tree in the current MST region. The switches that are not root bridges in the MST region adopt the maximum hops settings of their root bridges.

Configuration procedure

Table 177 Configure the maximum hops for an MST region

Operation	Command	Description
Enter system view	**system-view**	-
Configure the maximum hops for the MST region	**stp max-hops** *hops*	Required By default, the maximum hops of an MST region are 20.

Note that only the maximum hops settings on the switches operating as region roots can limit the size of the MST region.

Configuration example

Configure the maximum hops of the MST region to be 30 (assuming that the current switch operates as the region root).

```
<SW7750> system-view
[SW7750] stp max-hops 30
```

Network Diameter Configuration

In a switched network, any two switches can communicate with each other through a path, on which there may be some other switches. The network diameter of a network is measured by the number of switches; it equals the number of the switches on the longest path (that is, the path contains the maximum number of switches).

Configuration procedure

Table 178 Configure the network diameter for a network

Operation	Command	Description
Enter system view	**system-view**	-
Configure the network diameter for a network	**stp bridge-diameter** *bridgenumber*	Required The default network diameter of a network is 7.

The network diameter parameter indicates the size of a network. The larger the network diameter is, the larger the network size is.

After you configure the network diameter of a switched network, A MSTP-enabled switch adjusts its Hello time, Forward delay, and Max age settings accordingly.

The network diameter setting only applies to CIST; it is invalid for MSTIs.

Configuration example

Configure the network diameter of the switched network to 6.

```
<SW7750> system-view
[SW7750] stp bridge-diameter 6
```

MSTP Time-related Configuration

You can configure three MSTP time-related parameters for a switch: Forward delay, Hello time, and Max age.

- The Forward delay parameter sets the delay of state transition.

Link problems occurred in a network results in the spanning trees being regenerated and original spanning tree structures being changed. As the newly generated configuration BPDUs cannot be propagated across the entire network immediately when the new spanning trees are generated, loops may occur if the new root ports and designated ports begin to forward packets immediately.

This can be avoided by adopting a state transition mechanism. With this mechanism, newly selected root ports and designated ports undergo an intermediate state before they begin to forward packets. That is, it costs these ports a period (specified by the Forward delay parameter) for them to turn to the forwarding state. The period ensures that the newly generated configuration BPDUs to propagate across the entire network.

- The Hello time parameter is for link testing.

A switch regularly sends hello packets to other switches in the interval specified by the Hello time parameter to test the links.

- The Max age parameter is used to judge whether or not a configuration BPDU is obsolete. Obsolete configuration BPDUs will be discarded.

Configuration procedure

Table 179 Configure MSTP time-related parameters

Operation	Command	Description
Enter system view	**system-view**	-
Configure the Forward delay parameter	**stp timer forward-delay** *centiseconds*	Required The Forward delay parameter defaults to 1,500 centiseconds (15 seconds).
Configure the Hello time parameter	**stp timer hello** *centiseconds*	Required The Hello time parameter defaults to 200 centiseconds (2 seconds).
Configure the Max age parameter	**stp timer max-age** *centiseconds*	Required The Max age parameter defaults to 2,000 centiseconds (20 seconds).

All switches in a switched network adopt the three time-related parameters configured on the CIST root bridge.



CAUTION:

- *The Forward delay parameter and the network diameter are correlated. Normally, a large network diameter corresponds to a large Forward delay. A too small Forward delay parameter may result in temporary redundant paths. And a too large Forward delay parameter may cause a network unable to resume the normal state in time after changes occurred to the network. The default is recommended.*
- *An adequate Hello time parameter enables a switch to be aware of link problems in time without occupying too much network resources. A too large Hello time parameter may result in normal links being regarded as invalid when packets get lost on them, which in turn results in spanning trees being regenerated. And a too small Hello time parameter may result in duplicated configuration BPDUs being sent frequently, which increases the work load of the switches and wastes network resources. The default is recommended.*
- *As for the Max age parameter, if it is too small, network congestions may be falsely regarded as link problems, which results in spanning trees being frequently regenerated. If it is too large, link problems may be unable to be found in time, which in turn handicaps spanning trees being regenerated in time and makes the network less adaptive. The default is recommended.*

As for the configuration of these three time-related parameters (that is, the Hello time, Forward delay, and Max age parameters), the following formulas must be met to prevent network jitter.

2 x (Forward delay - 1 second) >= Max age

Max age >= 2 x (Hello time + 1 second)

You are recommended to specify the network diameter of the switched network and the Hello time by using the **stp root primary** or **stp root secondary** command. After that, the three proper time-related parameters are determined automatically.

Configuration example

Configure the Forward delay parameter to be 1,600 centiseconds, the Hello time parameter to be 300 centiseconds, and the Max age parameter to be 2,100 centiseconds (assuming that the current switch operates as the CIST root bridge).

```
<SW7750> system-view
[SW7750] stp timer forward-delay 1600
[SW7750] stp timer hello 300
[SW7750] stp timer max-age 2100
```

Timeout Time Factor Configuration

A switch regularly sends protocol packets to its neighboring devices at the interval specified by the Hello time parameter to test the links. Normally, a switch regards its upstream switch faulty if the former does not receive any protocol packets from the latter in a period three times of the Hello time and then initiates the spanning tree regeneration process.

Spanning trees may be regenerated even in a steady network if an upstream switch continues to be busy. You can configure the timeout time factor to a larger number to avoid this. Normally, the timeout time can be four or more times of the Hello time. For a steady network, the timeout time can be five to seven times of the Hello time.

Configuration procedure

Table 180 Configure timeout time factor

Operation	Command	Description
Enter system view	**system-view**	-
Configure the timeout time factor for the switch	**stp timer-factor** *number*	Required The timeout time factor defaults to 3.

Configuration example

Configure the timeout time factor to be 6.

```
<SW7750> system-view
[SW7750] stp timer-factor 6
```

Maximum Transmitting Speed Configuration

The maximum transmitting speed of a port specifies the maximum number of configuration BPDUs a port can transmit in a period specified by the Hello time

parameter. It depends on the physical state of the port and network structure. You can configure this parameter according to the network.

Configuration procedure (in system view)

Table 181 Configure the maximum transmitting speed for specified ports in system view

Operation	Command	Description
Enter system view	**system-view**	-
Configure the maximum transmitting speed for specified ports	**stp interface** *interface-list* **transmit-limit** *packetnum*	Required The maximum transmitting speed of all Ethernet ports on a switch defaults to 10.

Configuration procedure (in Ethernet port view)

Table 182 Configure the maximum transmitting speed in Ethernet port view

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Configure the maximum transmitting speed	**stp transmit-limit** *packetnum*	Required The maximum transmitting speed of all Ethernet ports on a switch defaults to 10.

As the maximum transmitting speed parameter determines the number of the configuration BPDUs transmitted in each Hello time, set it to a proper value to avoid MSTP from occupying too many network resources. The default is recommended.

Configuration example

Set the maximum transmitting speed of Ethernet1/0/1 port to 5.

- Configure the maximum transmitting speed in system view.

```
<SW7750> system-view
[SW7750] stp interface ethernet1/0/1 transmit-limit 5
```

- Configure the maximum transmitting speed in Ethernet port view.

```
<SW7750> system-view
[SW7750] interface ethernet1/0/1
[SW7750-Ethernet1/0/1] stp transmit-limit 5
```

Edge Port Configuration

Edge ports are ports that neither directly connects to other switches nor indirectly connects to other switches through network segments. After a port is configured as an edge port, rapid transition is applicable to the port. That is, when the port changes from blocking state to forwarding state, it does not have to wait for a delay.

You can configure a port as an edge port in the following two ways.

Configuration procedure (in system view)

Table 183 Configure a port as an edge port (in system view)

Operation	Command	Description
Enter system view	**system-view**	-
Configure the specified ports as edge ports	**stp interface** *interface-list* **edged-port enable**	Required By default, all the Ethernet ports of a switch are non-edge ports.

Configuration procedure (in Ethernet port view)

Table 184 Configure a port as an edge port (in Ethernet port view)

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Configure the port as an edge port	**stp edged-port enable**	Required By default, all the Ethernet ports of a switch are non-edge ports.

On a switch with BPDU protection not enabled, an edge port becomes a non-edge port again once it receives a BPDU from another port.



You are recommended to configure the Ethernet ports connected directly to terminals as edge ports and enable the BPDU protection function as well. This not only enables these ports to transit to forwarding state rapidly but also secures your network.

Configuration example

Configure port Ethernet1/0/1 as an edge port.

1 Configure in system view.

```
<SW7750> system-view
[SW7750] stp interface ethernet1/0/1 edged-port enable
```

2 Configure in Ethernet port view.

```
<SW7750> system-view
[SW7750] interface ethernet1/0/1
[SW7750-Ethernet1/0/1] stp edged-port enable
```

Point-to-point Link-Related Configuration

A point-to-point link directly connects two switches. If the roles of the two ports at the two ends of a point-to-point link meet certain criteria, the two ports can transit to the forwarding state rapidly by exchanging synchronization packets, eliminating the forwarding delay.

You can specify whether or not the link connected to a port is a point-to-point link in one of the following two ways.

Configuration procedure (in system view)

Table 185 Specify whether or not the links connected to the specified ports are point-to-point links (in system view)

Operation	Command	Description
Enter system view	**system-view**	-
Specify whether or not the links connected to the specified ports are point-to-point links	**stp interface** *interface-list* **point-to-point** { **force-true** | **force-false** | **auto** }	Required The **auto** keyword is adopted by default. The **force-true** keyword specifies that the links connected to the specified ports are point-to-point links. The **force-false** keyword specifies that the links connected to the specified ports are not point-to-point links. The **auto** keyword specifies to automatically determine whether or not the links connected to the specified ports are point-to-point links.

Configuration procedure (in Ethernet port view)

Table 186 Specify whether or not the link connected to a specific port is a point-to-point link (in Ethernet port view)

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Specify whether or not the link connected to the port is a point-to-point link	**stp point-to-point** { **force-true** | **force-false** | **auto** }	Required The **auto** keyword is adopted by default. The **force-true** keyword specifies that the link connected to the port is a point-to-point link. The **force-false** keyword specifies that the link connected to the port is not a point-to-point link. The **auto** keyword specifies to automatically determine whether or not the link connected to the port is a point-to-point link.



Among aggregated ports, you can only configure the links of master ports as point-to-point links.

If an auto-negotiating port operates in full duplex mode after negotiation, you can configure the link of the port as a point-to-point link.

After you configure the link of a port as a point-to-point link, the configuration applies to all spanning tree instances. If the actual physical link of a port is not a point-to-point link and you forcibly configure the link as a point-to-point link, temporary loops may be incurred.

Configuration example

Configure the link connected to port Ethernet1/0/1 as a point-to-point link.

1 Configure in system view.

```
<SW7750> system-view
[SW7750] stp interface ethernet1/0/1 point-to-point force-true
```

2 Configure in Ethernet port view.

```
<SW7750> system-view
[SW7750] interface ethernet1/0/1
[SW7750-Ethernet1/0/1] stp point-to-point force-true
```

MSTP Configuration

Configuration procedure

Table 187 Enable MSTP in system view

Operation	Command	Description
Enter system view	**system-view**	-
Enable MSTP	**stp enable**	Required MSTP is disabled by default.
Disable MSTP on specified ports	**stp interface** *interface-list* **disable**	Optional By default, MSTP is enabled on all ports after you enable MSTP in system view. To enable a switch to operate more flexibly, you can disable MSTP on specific ports. As MSTP-disabled ports do not participate in spanning tree generation, this operation saves CPU resources.

Table 188 Disable MSTP in Ethernet port view

Operation	Command	Description
Enter system view	**system-view**	-
Enable MSTP	**stp enable**	Required MSTP is disabled by default.
Enter Ethernet port view	**Interface** *interface-type interface-number*	-
Disable MSTP on the port	**stp disable**	Optional By default, MSTP is enabled on all ports after you enable MSTP in system view. To enable a switch to operate more flexibly, you can disable MSTP on specific ports. As MSTP-disabled ports do not participate in spanning tree generation, this operation saves CPU resources.

Other MSTP-related settings can take effect only after MSTP is enabled on the switch.

Configuration example

Enable MSTP on the switch and disable MSTP on Ethernet1/0/1 port.

1 Configure in system view.

```
<SW7750> system-view
[SW7750] stp enable
[SW7750] stp interface ethernet1/0/1 disable
```

2 Configure in Ethernet port view.

```
<SW7750> system-view
[SW7750] stp enable
[SW7750] interface ethernet1/0/1
[SW7750-Ethernet1/0/1] stp disable
```

Leaf Node Configuration

Table 189 lists MSTP-related configurations about leaf nodes.

Table 189 Leaf node configuration

Operation	Remarks	Related section
MSTP configuration	Required To prevent network topology jitter caused by other related configurations, you are recommended to enable MSTP after performing other configurations.	"MSTP Configuration" on page 258
MST region configuration	Required	"MST Region Configuration" on page 247
MSTP operation mode configuration	Optional	"MSTP Operation Mode Configuration" on page 250
Timeout time factor configuration	Optional	"Timeout Time Factor Configuration" on page 254
Maximum transmitting speed configuration	Optional The default is recommended.	"Maximum Transmitting Speed Configuration" on page 254
Edge port configuration	Optional	"Edge Port Configuration" on page 255
Path cost configuration	Optional	"Path Cost Configuration" on page 260
Port priority configuration	Optional	"Port Priority Configuration" on page 262
Point-to-point link related configuration	Optional	"Point-to-point Link-Related Configuration" on page 256

In a network that contains switches with both GVRP and MSTP employed, GVRP packets are forwarded along the CIST. If you want to broadcast packets of a specific VLAN through GVRP, be sure to map the VLAN to the CIST when configuring the MSTP VLAN mapping table (The CIST of a network is the spanning tree instance numbered 0.)

Prerequisites The status of the switches in the spanning trees is determined. That is, the status (root, branch, or leaf) of each switch in each spanning tree instance is determined.

MST Region Configuration

Refer to "MST Region Configuration" on page 247.

MSTP Operation Mode Configuration

Refer to "MSTP Operation Mode Configuration" on page 250.

Timeout Time Factor Configuration

Refer to "Timeout Time Factor Configuration" on page 254.

Maximum Transmitting Speed Configuration

Refer to "Maximum Transmitting Speed Configuration" on page 254.

Edge Port Configuration

Refer to "Edge Port Configuration" on page 255.

Path Cost Configuration

The path cost parameters reflects the link rates on ports. For a port on an MSTP-enabled switch, the path cost may differ with spanning tree instance. You can enable flows of different VLANs to travel along different physical links by configuring appropriate path costs on ports, so that load balancing can be achieved by VLANs.

Path cost can be determined by switch or through manual configuration.

Standards for calculating path costs of ports

Currently, a switch can calculate the path costs of ports based on one of the following standards:

- **dot1d-1998**: Adopts the IEEE 802.1D-1998 standard to calculate the default path costs of ports.
- **dot1t**: Adopts the IEEE 802.1t standard to calculate the default path costs of ports.
- **legacy**: Adopts the standard defined by private to calculate the default path costs of ports.

Table 190 Specify the standard for calculating path costs

Operation	Command	Description
Enter system view	**system-view**	-
Specify the standard to be used to calculate the default path costs of the links connected to the ports of the switch	**stp pathcost-standard** { **dot 1d-1998** | **dot1t** | **legacy** }	Optional By default, the legacy standard is used to calculate the default path costs.

Table 191 Transmission speeds and the corresponding path costs

Transmission speed	Operation mode (half-/full-duplex)	802.1D-1998	IEEE 802.1t	Proprietary standard
0	-	65,535	200,000,000	200,000

Table 191 Transmission speeds and the corresponding path costs

Transmission speed	Operation mode (half-/full-duplex)	802.1D-1998	IEEE 802.1t	Proprietary standard
10 Mbps	Half-duplex/Full-duplex	100	200,000	2,000
	Aggregated link 2 ports	95	1,000,000	1,800
	Aggregated link 3 ports	95	666,666	1,600
	Aggregated link 4 ports	95	500,000	1,400
100 Mbps	Half-duplex/Full-duplex	19	200,000	200
	Aggregated link 2 ports	15	100,000	180
	Aggregated link 3 ports	15	66,666	160
	Aggregated link 4 ports	15	50,000	140
1,000 Mbps	Full-duplex	4	200,000	20
	Aggregated link 2 ports	3	10,000	18
	Aggregated link 3 ports	3	6,666	16
	Aggregated link 4 ports	3	5,000	14
10 Gbps	Full-duplex	2	200,000	2
	Aggregated link 2 ports	1	1,000	1
	Aggregated link 3 ports	1	666	1
	Aggregated link 4 ports	1	500	1

Normally, the path cost of a port operating in full-duplex mode is slightly less than that of the port operating in half-duplex mode.

When calculating the path cost of an aggregated link, the 802.1D-1998 standard does not take the number of the ports on the aggregated link into account, whereas the 802.1T standard does. The following formula is used to calculate the path cost of an aggregated link:

Path cost = 200,000,/ link transmission speed,

Where the link transmission speed is the sum of the speeds of the unblocked ports on the aggregated link, which is measured in 100 Kbps.

Configuring the path costs of ports

Table 192 Configure the path cost for specified ports in system view

Operation	Command	Description
Enter system view	**system-view**	-
Configure the path cost for specified ports	**stp interface** *interface-list* [**instance** instance-id] **cost** *cost*	Required A MSTP-enabled switch can calculate path costs for all its ports automatically.

Table 193 Configure the path cost for a port in Ethernet port view

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-

Table 193 Configure the path cost for a port in Ethernet port view

Operation	Command	Description
Configure the path cost for the port	**stp** [**instance** *instance-id*] **cost** *cost*	Required A MSTP-enabled switch can calculate path costs for all its ports automatically.

Changing the path cost of a port may change the role of the port and put it in state transition. Executing the **stp cost** command with the *instance-id* argument being 0 sets the path cost on the CIST for the port.

Configuration example (A)

Configure the path cost of Ethernet1/0/1 port in spanning tree instance 1 to be 2,000.

1 Configure in system view.

```
<SW7750> system-view
[SW7750] stp interface ethernet1/0/1 instance 1 cost 2000
```

2 Configure in Ethernet port view.

```
<SW7750> system-view
[SW7750] interface ethernet1/0/1
[SW7750-Ethernet1/0/1] stp instance 1 cost 2000
```

Configuration example (B)

Change the path cost of Ethernet1/0/1 port in spanning tree instance 1 to the default one calculated with the IEEE 802.1D-1998 standard.

```
<SW7750> system-view
[SW7750] stp pathcost-standard dot1d-1998
```

Port Priority Configuration

Port priority is an important criterion on determining the root port. In the same condition, ports with smaller port priority values are more potential to become the root port than those with bigger priority values.

A port on a MSTP-enabled switch can have different port priorities and play different roles in different spanning tree instances. This enables packets of different VLANs to be forwarded along different physical paths, so that load balancing can be achieved by VLANs.

You can configure port priority in the following two ways.

Configuring port priority in system view

Table 194 Configure port priority for specified ports in system view

Operation	Command	Description
Enter system view	**system-view**	-
Configure port priority for specified ports	**stp interface** *interface-list* **instance** *instance-id* **port priority** *priority*	Required The default port priority is 128.

Configuring port priority in Ethernet port view

Table 195 Configure port priority for a specified port in Ethernet port view

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Configure port priority for the port	**stp** [**instance** *instance-id*] **port priority** *priority*	Required. The default port priority is 128.

Changing port priority of a port may change the role of the port and put the port into state transition.

A smaller port priority value indicates a higher possibility for the port to become the root port. If all the ports of a switch have the same port priority value, the port priorities are determined by the port indexes. Changing the priority of a port will cause spanning tree regeneration.

You can configure port priorities according to actual networking requirements.

Configuration example

Configure the port priority of Ethernet1/0/1 port in spanning tree instance 1 to be 16.

1 Configure in system view.

```
<SW7750> system-view
[SW7750] stp interface ethernet1/0/1 instance 1 port priority 16
```

2 Configure in Ethernet port view.

```
<SW7750> system-view
[SW7750] interface ethernet1/0/1
[SW7750-Ethernet1/0/1] stp instance 1 port priority 16
```

Point-to-point Link-Related Configuration

Refer to "Point-to-point Link-Related Configuration" on page 256.

MSTP Configuration

Refer to "MSTP Configuration" on page 258.

The mCheck Configuration

As mentioned previously, ports on an MSTP-enabled switch can operate in three modes: STP-compatible, RSTP-compatible, and MSTP.

A port on an MSTP-enabled switch operating as an upstream switch transits to the STP-compatible mode when it has an STP-enabled switch connected to it. When the STP enabled downstream switch is then replaced by an MSTP-enabled switch, the port cannot automatically transit to the MSTP mode. It remains in the STP-compatible mode. In this case, you can force the port to transit to the MSTP mode by performing the mCheck operation on the port.

Similarly, a port on an RSTP-enabled switch operating as an upstream switch transits to the STP-compatible mode when it has an STP enabled switch connected to it. When the STP enabled downstream switch is then replaced by an

MSTP-enabled switch, the port cannot automatically transit to the MSTP operation mode. It remains in the STP-compatible mode. In this case, you can force the port to transit to the MSTP mode by performing the mCheck operation on the port.

Prerequisites MSTP runs normally on the switch.

Configuration Procedure You can perform the mCheck operation in the following two ways.

Performing the mCheck operation in system view

Table 196 Perform the mCheck operation in system view

Operation	Command	Description
Enter system view	**System-view**	-
Perform the mCheck operation	**stp** [**interface** *interface-list*] **mcheck**	Required

Performing the mCheck operation in Ethernet port view

Table 197 Perform the mCheck operation in Ethernet port view

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Perform the mCheck operation	**stp mcheck**	Required

Configuration Example # Perform the mCheck operation on Ethernet1/0/1 port

- Configure in system view.

```
<SW7750> system-view
[SW7750] stp interface ethernet1/0/1 mcheck
```

- Configure in Ethernet port view.

```
<SW7750> system-view
[SW7750] interface ethernet1/0/1
[SW7750-Ethernet1/0/1] stp mcheck
```

Protection Function Configuration

Introduction The following protection functions are available on an MSTP-enabled switch: BPDU protection, root protection, loop guard, and topology change BPDU (TC-BPDU) attack guard.

BPDU protection

Normally, the access ports of the devices operating on the access layer directly connect to terminals (such as PCs) or file servers. These ports are usually configured as edge ports to achieve rapid transition. But they resume non-edge ports automatically upon receiving configuration BPDUs, which causes spanning tree regeneration and network topology jitter.

Normally, no configuration BPDU will reach edge ports. But malicious users can attack a network by sending configuration BPDUs deliberately to edge ports to cause network jitter. You can prevent this type of attacks by utilizing the BPDU protection function. With this function enabled on a switch, the switch shuts down the edge ports that receive configuration BPDUs and then reports these cases to the administrator. If a port is shut down, only the administrator can restore it.

Root protection

A root bridge and its secondary root bridges must reside in the same region. A CIST and its secondary root bridges are usually located in the high-bandwidth core region. Configuration errors or attacks may result in configuration BPDUs with their priorities higher than that of a root bridge, which causes new root bridge to be elected and network topology jitter to occur. In this case, flows that should travel along high-speed links may be led to low-speed links, and network congestion may occur.

You can avoid this by utilizing the root protection function. Ports with this function enabled can only be kept as designated ports in all spanning tree instances. When a port of this type receives configuration BPDUs with higher priorities, it changes to discarding state (rather than becomes a non-designated port) and stops forwarding packets (as if it is disconnected from the link). It resumes the normal state if it does not receive any configuration BPDUs with higher priorities for a specified period.

Loop guard

A switch maintains the states of the root port and other blocked ports by receiving and processing BPDUs from the upstream switch. These BPDUs may get lost because of network congestions and link failures. If a switch does not receive BPDUs from the upstream switch for certain period, the switch selects a new root port; the original root port becomes a designated port; and the blocked ports transit to forwarding state. This may cause loops in the network.

The loop guard function suppresses loops. With this function enabled, if link congestions or link failures occur, both the root port and the blocked ports become designated ports and change to be in the discarding state. In this case, they stop forwarding packets, and thereby loops can be prevented.

TC-BPDU attack guard

Generally, upon receiving a TC-BPDU, a switch removes its local MAC address table and then updates the ARP address table based on STP instances according to the updated MAC address table. If a malicious user forges TC-BPDUs to attack a switch, the switch will receive a large amount of TC-BPDUs in a short period, causing the switch busy in removing local MAC address tables and updating ARP address tables, which will affect STP calculation and occupy a large amount of network bandwidth. As a result, the CPU utilization stays high for the switch.

With the TC-BPDU guard function enabled, the switch performs the operation of removing its local MAC address table once after it receives a TC-BPDU, and triggers a timer at the same time, which expires after 10 seconds. Before the timer expires, the switch can only perform the operation of removing MAC address entries for up to six times. Such a mechanism prevents the switch from removing

MAC address tables frequently and negative effects to STP calculation and network stability.

You can use the **stp tc-protection threshold** command to set a threshold for the times of removing MAC address tables in a period. If the number of received TC-BPDUs is less than the specified upper threshold, the switch removes its MAC address table upon receiving a TC-BPDU. If the number of received TC-BPDUs is more than the specified upper threshold, the switch will remove its MAC address table for the times equal to the specified upper threshold. For example, if you set the upper threshold for the times for the switch to remove its MAC address table to 100 in the specific period, while the switch receives 200 TC-BPDUs in the period. In this case, the switch removes its MAC address table for only 100 times within the period.

CAUTION: *Among loop guard function, root protection function, and edge port setting, only one can be valid on a port at one time.*

BPDU Protection Configuration

Configuration prerequisites

MSTP is enabled on the current switch.

Configuration procedure

Table 198 Enable the BPDU guard function

Operation	Command	Description
Enter system view	**system-view**	-
Enable the BPDU guard function	**stp bpdu-protection**	Required The BPDU guard function is disabled by default.

Configuration example

Enable the BPDU guard function.

```
<SW7750> system-view
[SW7750] stp bpdu-protection
```

CAUTION: *As Gigabit ports of a Switch 7750 cannot be shut down, the BPDU guard function is not applicable to these ports even if you enable the BPDU guard function and specify these ports to be MSTP edge ports.*

Root Guard Configuration

Configuration prerequisites

MSTP is enabled on the current switch.

Configuration procedure

Table 199 Enable the root guard function in system view

Operation	Command	Description
Enter system view	**system-view**	-
Enable the root guard function on specified ports	**stp interface** *interface-list* **root-protection**	Required The root guard function is disabled by default.

Table 200 Enable the root guard function in Ethernet port view

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**Interface** *interface-type interface-number*	-
Enable the root guard function on current port	**stp root-protection**	Required The root guard function is disabled by default.

Configuration example

Enable the root guard function on Ethernet1/0/1 port.

1 Configure in system view.

```
<SW7750> system-view
[SW7750] stp interface ethernet1/0/1 root-protection
```

2 Configure in Ethernet port view.

```
<SW7750> system-view
[SW7750] interface ethernet1/0/1
[SW7750-Ethernet1/0/1] stp root-protection
```

Loop Guard Configuration

Configuration prerequisites

MSTP is enabled on the current switch.

Configuration procedure

Table 201 Enable the Loop guard function in system view

Operation	Command	Description
Enter system view	**system-view**	-
Enable the loop guard function on specified ports	**stp interface** *interface-list* **loop-protection**	Required The loop prevention function is disabled by default.

Table 202 Enable the Loop guard function in Ethernet port view

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Enable the loop prevention function on the current port	**stp loop-protection**	Required The loop prevention function is disabled by default.

Configuration example

Enable loop prevention function on Ethernet1/0/1 port.

1 Configure in system view.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] stp interface ethernet1/0/1 loop-protection
```

2 Configure in Ethernet port view.

```
<SW7750> system-view
[SW7750] interface ethernet1/0/1
[SW7750-Ethernet1/0/1] stp loop-protection
```

TC-BPDU Attack Prevention Configuration

Configuration prerequisites

MSTP is enabled on the current switch.

Configuration procedure

Table 203 Enable the TC-BPDU attack prevention function

Operation	Command	Description
Enter system view	**system-view**	-
Enable the TC-BPDU attack prevention function	**stp tc-protection enable**	Required The TC-BPDU attack prevention function is enabled by default.
Configure the times for the switch to remove MAC address tables within 10 seconds	**stp tc-protection threshold** *number*	Optional

Configuration example

Enable the TC-BPDU attack prevention function

```
<SW7750> system-view
[SW7750] stp tc-protection enable
```

Configure the switch to remove MAC addresses for up to 5 times within 10 seconds.

```
<SW7750> system-view
[SW7750] stp tc-protection threshold 5
```

Digest Snooping Configuration

Introduction

According to IEEE 802.1s, two interconnected MSTP switches can interwork with each other through MSTIs in an MST region only when the two switches have the same MST region-related configuration. Interconnected MSTP switches determine whether or not they are in the same MST region by checking the configuration IDs of the BPDUs between them. (A configuration ID contains information such as region ID and configuration digest.)

As some partners' switches adopt proprietary spanning tree protocols, they cannot interwork with other switches in an MST region even if they are configured with the same MST region-related settings as other switches in the MST region.

This problem can be overcome by implementing the digest snooping feature. If a port on a Switch 7750 is connected to a partner's switch that has the same MST region-related configuration as its own but adopts a proprietary spanning tree protocol, you can enable digest snooping on the port. Then the Switch 7750 regards the partner's switch as in the same region; it records the configuration digests carried in the BPDUs received from the partner's switch, and put them in

the BPDUs to be send to the partner's switch. In this way, the Switch 7750s can interwork with the partners' switches in the same MST region.

Digest Snooping Configuration

Configure the digest snooping feature on a switch to enable it to interwork with other switches that adopt proprietary protocols to calculate configuration digests in the same MST region through MSTIs.

Prerequisites

The switch to be configured is connected to a partner's switch that adopts a proprietary spanning tree protocol. The MSTP network operates normally.

Configuration procedure

Table 204 Configure the digest snooping feature

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Enable the digest snooping feature	**stp config-digest-snooping**	Required The digest snooping feature is disabled on the port by default.
Return to system view	**Quit**	-
Enable the digest snooping feature globally	**stp config-digest-snooping**	Required The digest snooping feature is disabled globally by default.
Verify the above configuration	**display current-configuration**	You can execute this command in any view.



- *The digest snooping feature is needed only when your Switch 7750 is connected to partner's proprietary protocol-adopted switches.*
- *To enable the digest snooping feature successfully, you must first enable it on all the ports of your Switch 7750 that are connected to partner's proprietary protocol-adopted switches and then enable it globally.*
- *To enable the digest snooping feature, the interconnected switches must be configured with exactly the same MST region-related configurations (including region name, revision level, and VLAN-to-MSTI mapping).*
- *The digest snooping feature must be enabled on all the ports of your Switch 7750 that are connected to partners' proprietary protocol-adopted switches in the same MST region.*
- *With the digest snooping feature is enabled, the VLAN-to-MSTI mapping cannot be modified.*
- *The digest snooping feature is not applicable on MST region edge ports.*

Rapid Transition Configuration

Introduction

Designated ports on switches adopting RSTP or MSTP use the following two types of packets to implement rapid transition:

- Proposal packets: Packets sent by designated ports to request rapid transition
- Agreement packets: Packets used to acknowledge rapid transition requests

Both RSTP and MSTP switches can perform rapid transition operation on a designated port only when the port receives an agreement packet from the downstream switch. The difference between RSTP and MSTP switches are:

- An MSTP upstream switch sends agreement packets to the downstream switch; and an MSTP downstream switch sends an agreement packet to the upstream switch only after it receives an agreement packet from the upstream switch.
- A RSTP upstream switch does not send agreement packets to the downstream switch.

Figure 62 and Figure 63 illustrate the RSTP and MSTP rapid transition mechanisms.

Figure 62 The RSTP rapid transition mechanism

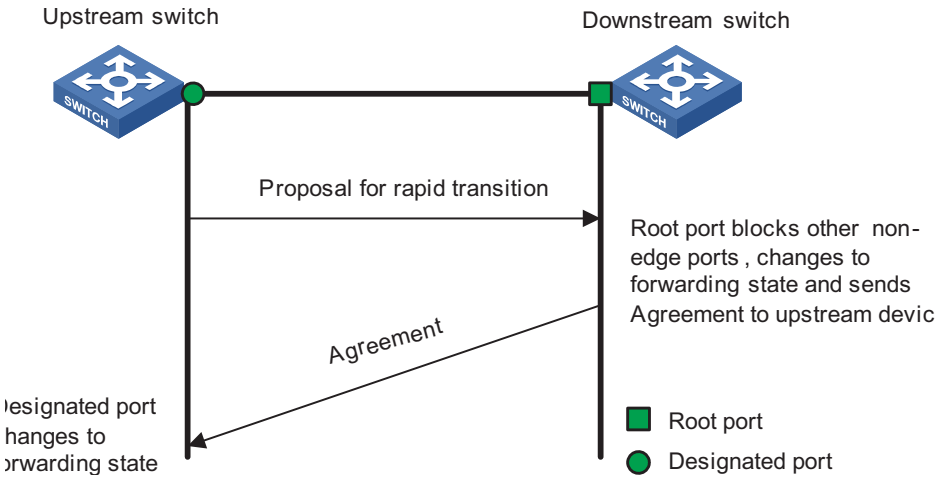
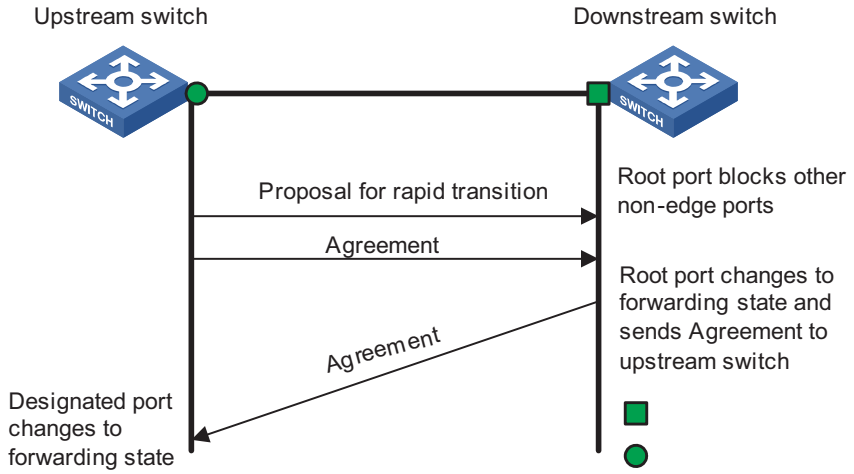


Figure 63 The MSTP rapid transition mechanism



Limitation on the combination of RSTP and MSTP exists to implement rapid transition. For example, when the upstream switch adopts RSTP, the downstream switch adopts MSTP and does not support RSTP-compatible mode, the root port

on the downstream switch receives no agreement packet from the upstream switch and thus sends no agreement packets to the upstream switch. As a result, the designated port of the upstream switch fails to transit rapidly and can only change to the Forwarding state after a period twice the Forward Delay.

Some partners' switches adopt proprietary spanning tree protocols that are similar to RSTP in the way to implement rapid transition on designated ports. When a switch of this kind operating as the upstream switch connects with the 3Com series switch running MSTP, the upstream designated port fails to change their states rapidly.

The rapid transition feature is developed to resolve this problem. When a 3Com series switch running MSTP is connected in the upstream direction to a partner's switch running proprietary spanning tree protocol, you can enable the rapid transition feature on the ports of the 3Com series switch operating as the downstream switch. Among these ports, those operating as the root ports will then send agreement packets to their upstream ports after they receive proposal packets from the upstream designated ports, instead of waiting for agreement packets from the upstream switch. This enables designated ports of the upstream switch to change their states rapidly.

Rapid Transition Configuration

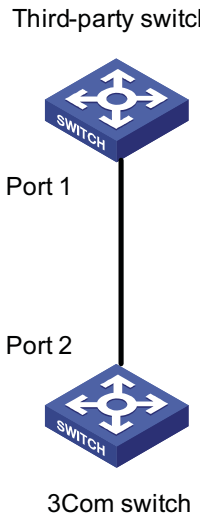
Prerequisites

As shown in Figure 64, a 3Com series switch is connected to a partner's switch. The former operates as the downstream switch, and the latter operates as the upstream switch. The network operates normally.

The upstream switch is running a proprietary spanning tree protocol that is similar to RSTP in the way to implement rapid transition on designated ports. Port 1 is a designated port.

The downstream switch is running MSTP. Port 2 is the root port.

Figure 64 Network diagram for rapid transition configuration



Configuration procedure

1 Configure the rapid transition feature in system view.

Table 205 Configure the rapid transition feature in system view

Operation	Command	Description
Enter system view	**system-view**	-
Enable the rapid transition feature	**stp interface** *interface-type interface-number* **no-agreement-check**	Required By default, the rapid transition feature is disabled on a port.

2 Configure in Ethernet port view.

Table 206 Configure the rapid transition feature in Ethernet port view

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Enable the rapid transition feature	**stp no-agreement-check**	Required By default, the rapid transition feature is disabled on a port.

- *The rapid transition feature can be enabled on root ports or alternate ports only.*
- *If you configure the rapid transition feature on the designated port, the feature does not take effect on the port.*

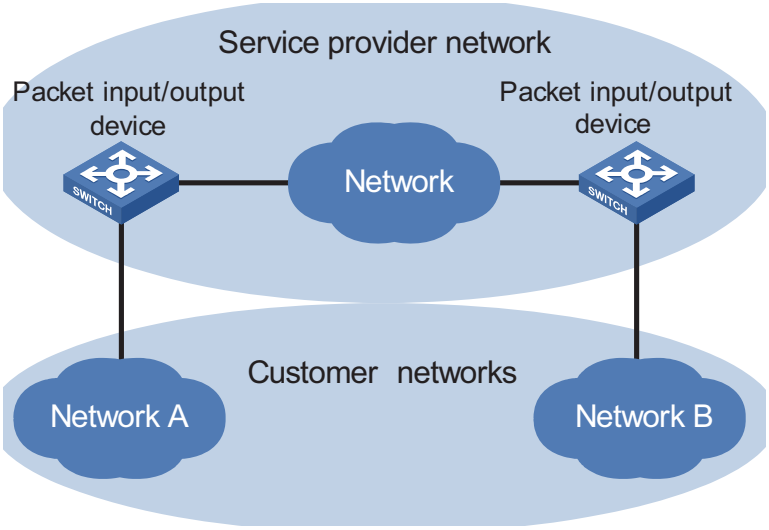
BPDU Tunnel Configuration

Introduction

The BPDU Tunnel function enables BPDUs to be transparently transmitted between geographically dispersed user networks through specified VLAN VPNs in operator's networks, through which spanning trees can be generated across these user networks and are independent of those of the operator's network.

As shown in Figure 65, the upper part is the operator's network, and the lower part is the user network. The operator's network comprises packet ingress/egress devices, and the user's network has networks A and B. On the operator's network, configure the arriving BPDU packets at the ingress to have MAC addresses in a special format, and reconvert them back to their original formats at the egress. This is how transparent transmission is implemented on the operator's network.

Figure 65 BPDU Tunnel network hierarchy



BPDU Tunnel Configuration

Configuration prerequisites

MSTP is enabled on the current switch.

Configuration procedure

Table 207 Configure the BPDU Tunnel function

Operation	Command	Description
Enter system view	**system-view**	-
Enable MSTP globally	**stp enable**	-
Enable the BPDU Tunnel function globally	**vlan-vpn tunnel**	Required
Enter Ethernet port view	**interface** *interface-type interface-number*	Make sure that you enter the Ethernet port view of the port for which you want to enable the BPDU Tunnel function.
Disable MSTP for the port	**stp disable**	-
Enable the VLAN VPN function for the Ethernet port	**vlan-vpn enable**	Required By default, the VLAN VPN function is disabled on all ports.

- *The BPDU Tunnel function can only be enabled on devices with STP enabled.*
- *The BPDU Tunnel function can only be enabled on access ports.*
- *To enable the BPDU Tunnel function, make sure the links between operator's networks are trunk links.*
- *If a fabric port exists on a switch, you cannot configure VLAN-VPN function on any port of the switch.*
- *As the VLAN-VPN function is unavailable on ports with 802.1x, GVRP, GMRP, STP, or NTDP enabled, the BPDU Tunnel function is not applicable to these ports.*

STP Maintenance Configuration

Introduction

In a large-scale network with MSTP enabled, there may be many MSTP instances, and so the status of a port may change frequently. In this case, maintenance personnel may expect that log/trap information is output to the log host when particular ports fail, so that they can check the status changes of those ports through alarm information.

Enabling Log/Trap Output for Ports of MSTP Instance

Table 208 Enable log/trap output for ports of MSTP instance

Operation	Command	Description
Enter system view	**system-view**	-
Enable log/trap output for the ports of a specified instance	**stp** [**instance** *instance-id*] **portlog**	Required By default, log/trap output is disabled for the ports of all instances.
Enable log/trap output for the ports of all instances	**stp portlog all**	Required By default, log/trap output is disabled for the ports of all instances.

Configuration Example

Enable log/trap output for the ports of instance 1.

```
<SW7750> system-view
[SW7750] stp instance 1 portlog
```

Enable log/trap output for the ports of all instances.

```
<SW7750> system-view
[SW7750] stp portlog all
```

MSTP Displaying and Debugging

You can verify the above configurations by executing the **display** commands in any view.

Execute the **reset** command in user view to clear MSTP statistics.

Table 209 Display and debug MSTP

Operation	Command
Display spanning tree-related information about the current switch	**display stp** [**instance** *instance-id*] [**interface** *interface-list* | **slot** *slot-number*] [**brief**]
Display region configuration	**display stp region-configuration**
Display information about the ports that are shut down by STP protection	**display stp portdown**
Display information about the ports that are blocked by STP protection	**display stp abnormalport**
Display information about the root port of the instance where the switch reside	**display stp root**
Clear MSTP-related statistics	**reset stp** [**interface** *interface-list*]

MSTP Implementation Example

Network requirements

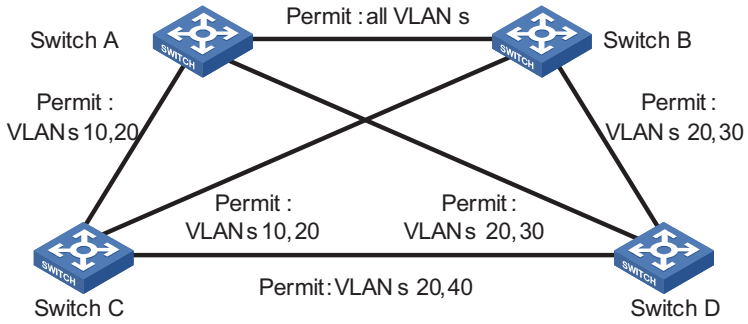
Implement MSTP in the network shown in Figure 66 to enable packets of different VLANs to be forwarded along different spanning tree instances. The detailed configurations are as follows:

- All switches in the network belong to the same MST region.
- Packets of VLAN 10, VLAN 30, VLAN 40, and VLAN 20 are forwarded along spanning tree instance 1, instance 3, instance 4, and instance 0 respectively.

In this network, Switch A and Switch B operate on the distribution layer; Switch C and Switch D operate on the access layer. VLAN 10 and VLAN 30 are limited in the distribution layer and VLAN 40 is limited in the access layer. Switch A and Switch B are configured as the root bridges of spanning tree instance 1 and spanning tree instance 3 respectively. Switch C is configured as the root bridge of spanning tree instance 4.

Network diagram

Figure 66 Network diagram for implementing MSTP



The "Permit:" shown in Figure 66 means the corresponding link permits packets of specific VLANs.

Configuration procedure

1 Configure Switch A.

Enter MST region view.

```
<SW7750> system-view
[SW7750] stp enable
[SW7750] stp region-configuration
```

Configure the MST region.

```
[SW7750-mst-region] region-name example
[SW7750-mst-region] instance 1 vlan 10
[SW7750-mst-region] instance 3 vlan 30
[SW7750-mst-region] instance 4 vlan 40
[SW7750-mst-region] revision-level 0
```

Activate the settings of the MST region.

```
[SW7750-mst-region] active region-configuration
```

Specify Switch A as the root bridge of spanning tree instance 1.

```
[SW7750] stp instance 1 root primary
```

2 Configure Switch B.

Enter MST region view.

```
<SW7750> system-view
[SW7750] stp region-configuration
```

Configure the MST region.

```
[SW7750-mst-region] region-name example
[SW7750-mst-region] instance 1 vlan 10
[SW7750-mst-region] instance 3 vlan 30
[SW7750-mst-region] instance 4 vlan 40
[SW7750-mst-region] revision-level 0
```

Activate the settings of the MST region.

```
[SW7750-mst-region] active region-configuration
```

Specify Switch B as the root bridge of spanning tree instance 3.

```
[SW7750] stp instance 3 root primary
```

3 Configure Switch C.

Enter MST region view.

```
<SW7750> system-view
[SW7750] stp region-configuration
```

Configure the MST region.

```
[SW7750-mst-region] region-name example
[SW7750-mst-region] instance 1 vlan 10
[SW7750-mst-region] instance 3 vlan 30
[SW7750-mst-region] instance 4 vlan 40
[SW7750-mst-region] revision-level 0
```

Activate the settings of the MST region.

```
[SW7750-mst-region] active region-configuration
```

Specify Switch C as the root bridge of spanning tree instance 4.

```
[SW7750] stp instance 4 root primary
```

- Configure Switch D.

Enter MST region view.

```
<SW7750> system-view
[SW7750] stp region-configuration
```

Configure the MST region.

```
[SW7750-mst-region] region-name example
[SW7750-mst-region] instance 1 vlan 10
[SW7750-mst-region] instance 3 vlan 30
[SW7750-mst-region] instance 4 vlan 40
[SW7750-mst-region] revision-level 0
```

Activate the settings of the MST region.

```
[SW7750-mst-region] active region-configuration
```

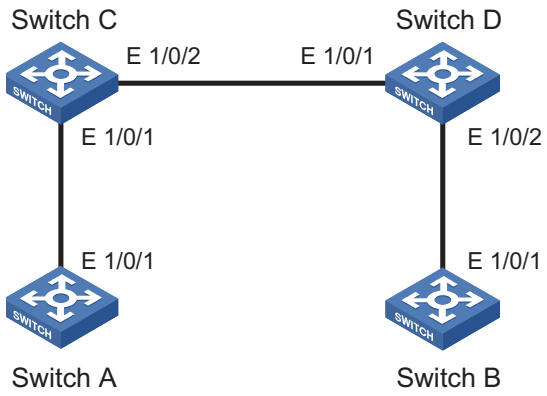
BPDU Tunnel Configuration Example

Network requirements

- Switch 7750s operate as the access devices of the operator's network, that is, Switch C and Switch D in the network diagram.
- S2000 series switches operate as the access devices of the user's network, that is, Switch A and Switch B in the network diagram.
- Switch C and Switch D connect to each other through the configured trunk port of the switch, and are enabled with the BPDU Tunnel function. Thereby transparent transmission is realized between the user's network and the operator's network.

Network diagram

Figure 67 Network diagram for BPDU Tunnel configuration



Configuration procedure

1 Configure Switch A.

Enable RSTP.

```
<SW7750> system-view
[SW7750] stp enable
```

Add port Ethernet1/0/1 to VLAN 10.

```
[SW7750] vlan 10
[SW7750-Vlan10] port Ethernet 1/0/1
```

2 Configure Switch B.

Enable RSTP.

```
<SW7750> system-view
[SW7750] stp enable
```

Add port Ethernet1/0/1 to VLAN 10.

```
[SW7750] vlan 10
[SW7750-Vlan10] port Ethernet 1/0/1
```

3 Configure Switch C.

Enable MSTP.

```
<SW7750> system-view
[SW7750] stp enable
```

Enable the BPDU Tunnel function.

```
[SW7750] vlan-vpn tunnel
```

Add port Ethernet1/0/1 to VLAN 10.

```
[SW7750] vlan 10
[SW7750-Vlan10] port Ethernet 1/0/1
[SW7750-Vlan10] quit
```

Disable STP on port Ethernet1/0/1 and then enable the VLAN-VPN function on it.

```
[SW7750] interface Ethernet 1/0/1
[SW7750-Ethernet1/0/1] port access vlan 10
[SW7750-Ethernet1/0/1] stp disable
[SW7750-Ethernet1/0/1] vlan-vpn enable
[SW7750-Ethernet1/0/1] quit
```

Configure port Ethernet1/0/2 as a trunk port.

```
[SW7750] interface Ethernet 1/0/2
[SW7750-Ethernet1/0/2] port link-type trunk
```

Add the trunk port to all VLANs.

```
[SW7750-Ethernet1/0/2] port trunk permit vlan all
```

Configure Switch D.

Enable MSTP.

```
<SW7750> system-view
[SW7750] stp enable
```

Enable the BPDU Tunnel function.

```
[SW7750] vlan-vpn tunnel
```

Add port Ethernet1/0/2 to VLAN 10.

```
[SW7750] vlan 10
[SW7750-Vlan10] port Ethernet 1/0/2
```

Disable STP on port Ethernet1/0/2 and then enable the VLAN-VPN function on it.

```
[SW7750] interface Ethernet 1/0/2
[SW7750-Ethernet1/0/2] port access vlan 10
[SW7750-Ethernet1/0/2] stp disable
[SW7750-Ethernet1/0/2] vlan-vpn enable
[SW7750-Ethernet1/0/2] quit
```

Configure port Ethernet1/0/1 as a trunk port.

```
[SW7750] interface Ethernet 1/0/1
[SW7750-Ethernet1/0/1] port link-type trunk
```

Add the trunk port to all VLANs.

```
[SW7750-Ethernet1/0/1] port trunk permit vlan all
```

31 IP ROUTING PROTOCOL OVERVIEW

When running a routing protocol, the Ethernet switch also functions as a router. The word "router" and the router icons covered in the following text represent routers in common sense and Ethernet switches running a routing protocol. To improve readability, this will not be mentioned again in this manual.

Introduction to IP Route and Routing Table

IP Route

Routers are used for route selection on the Internet. As a router receives a packet, it selects an appropriate route (through a network) according to the destination address of the packet and forwards the packet to the next router. The last router on the route is responsible for delivering the packet to the destination host.

Routing Table

The key for a router to forward packets is the routing table. Each router maintains a routing table. Each entry in this table contains an IP address that represents a host/subnet and specifies which physical port on the router should be used to forward the packets destined for the host/subnet. And the router forwards those packets through this port to the next router or directly to the destination host if the host is on a network directly connected to the router.

Each entry in a routing table contains:

- Destination address: It identifies the address of the destination host or network of an IP packet.
- Network mask: Along with the destination address, it identifies the address of the network segment where the destination host or router resides. By performing "logical AND" between destination address and network mask, you can get the address of the network segment where the destination host or router resides. For example, if the destination address is 129.102.8.10 and the mask is 255.255.0.0, the address of the network segment where the destination host or router resides is 129.102.0.0.A mask consists of some consecutive 1s, represented either in dotted decimal notation or by the number of the consecutive 1s in the mask.
- Output interface: It indicates through which interface IP packets should be forwarded to reach the destination.
- Next hop address: It indicates the next router that IP packets will pass through to reach the destination.
- Preference of the route added to the IP routing table: There may be multiple routes with different next hops to the same destination. These routes may be discovered by different routing protocols, or be manually configured static

routes. The one with the highest preference (the smallest numerical value) will be selected as the current optimal route.

According to different destinations, routes fall into the following categories:

- Subnet route: The destination is a subnet.
- Host route: The destination is a host.

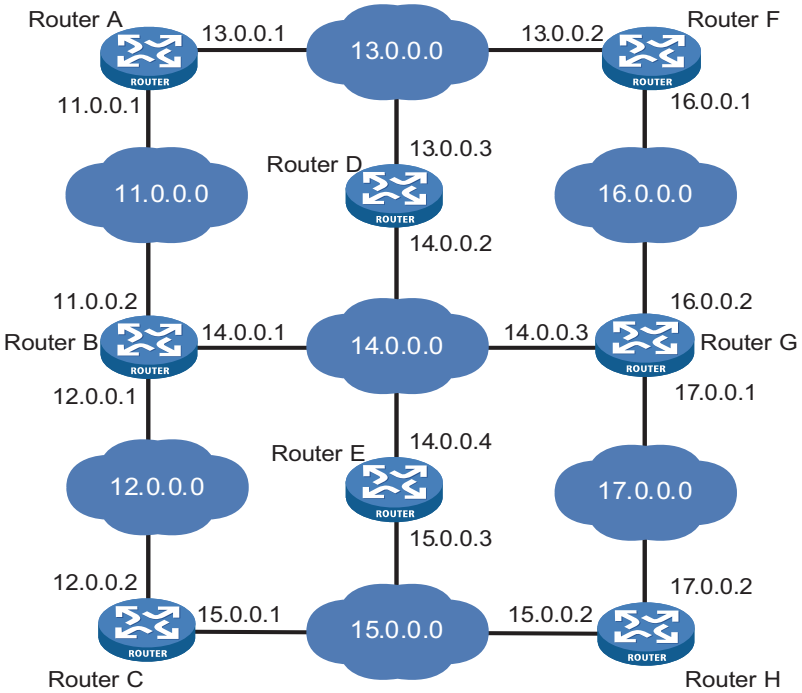
In addition, according to whether the network where the destination resides is directly connected to the router, routes falls into the following categories:

- Direct route: The router is directly connected to the network where the destination resides.
- Indirect route: The router is not directly connected to the network where the destination resides.

In order to avoid an oversized routing table, you can set a default route. All the packets for which the router fails to find a matching entry in the routing table will be forwarded through this default route.

As shown in Figure 68, the number in each network cloud indicates the network address and "R" represents a router. Router G is connected to three networks, and so it has three IP addresses and three physical ports. Its routing table is shown in Figure 68.

Figure 68 Routing table



Destination Network	Nexthop	Interface
11.0.0.0	14.0.0.1	3
12.0.0.0	14.0.0.1	3
13.0.0.0	16.0.0.1	2
14.0.0.0	14.0.0.3	3
15.0.0.0	17.0.0.2	1
16.0.0.0	16.0.0.2	2
17.0.0.0	17.0.0.1	1

The Switch 7750 Ethernet Switches (hereinafter referred to as the Switch 7750) support the configuration of static routes as well as a series of dynamic routing protocols such as RIP, OSPF and BGP. Moreover, the switches in operation can automatically obtain some direct routes according to interface status and user configuration.

Routing Management Policy

On a Switch 7750, you can manually configure a static route to a certain destination, or configure a dynamic routing protocol to make the switch interact with other routers in the internetwork and find routes by routing algorithm. On a Switch 7750, the static routes configured by the user and the dynamic routes discovered by routing protocols are managed uniformly. The static routes and the routes learned or configured by different routing protocols can also be shared among routing protocols.

Routing Protocols and Preferences

Different routing protocols may discover different routes to the same destination, but only one route among these routes and the static routes is optimal. In fact, at any given moment, only one routing protocol can determine the current route to a specific destination. Routing protocols (including static routing) are endowed with different preferences. When there are multiple routing information sources, the route discovered by the routing protocol with the highest preference will become the current route. Routing protocols and their default route preferences (the smaller the value, the higher the preference is) are shown in Table 210.

In the table, "0" is used for directly connected routes, and "255" is used for routes from untrusted source.

Table 210 Routing protocols and corresponding route preferences

Routing protocol or type	Preference of the corresponding route
DIRECT	0
OSPF	10
IS-IS	15
STATIC	60
RIP	100
OSPF ASE	150
OSPF NSSA	150
UNKNOWN	255
IBGP	256
EBGP	256

Except for direct routing, you can manually configure the preferences of various dynamic routing protocols as required. In addition, you can configure different preferences for different static routes.

Traffic Sharing and Route Backup

Traffic sharing

The Switch 7750 support multi-route mode, allowing the configuration of multiple routes that reach the same destination and have the same preference. The same destination can be reached via multiple different routes, whose preferences are equal. When there is no route with a higher preference to the same destination, the multiple routes will be adopted. Then, the packets destined for the same destination will be forwarded through these routes in turn to implement traffic sharing.

Route backup

The Switch 7750 support route backup. When the main route fails, the system automatically switches to a backup route to improve network reliability.

To achieve route backup, you can configure multiple routes to the same destination according to actual situation. One of the routes has the highest preference and is called primary route. The other routes have descending preferences and are called backup routes. Normally, the router sends data through the main route. When line failure occurs on the main route, the main route will hide itself and the router will choose the one whose preference is the highest among the remaining backup routes as the path to send data. In this way, the switchover from the main route to a backup route is implemented. When the main route recovers, the router will restore it and re-select a route. And, as the main route has the highest preference, the router will choose the main route to send data. This process is the automatic switchover from the backup route to the main route.

Routes Shared Between Routing Protocols

As the algorithms of various routing protocols are different, different routing protocols may discover different routes. This brings about the problem of how to share the discovered routes between routing protocols. The Switch 7750 can import (with the **import-route** command) the routes discovered by one routing protocol to another routing protocol. Each protocol has its own route redistribution mechanism. For detailed information, refer to "Importing Routes" on page 357.

32 STATIC ROUTE CONFIGURATION

Introduction to Static Route

Static Route

Static routes are special routes. They are manually configured by the administrator. By configuring static routes, you can build an interconnecting network. The problem for such configuration is when a fault occurs on the network, a static route cannot change automatically to steer away from the fault point without the help of the administrator.

In a relatively simple network, you only need to configure static routes to make routers work normally. Proper configuration and usage of static routes can improve network performance and ensure sufficient bandwidth for important applications.

Static routes are divided into three types:

- Reachable route: normal route. If a static route to a destination is of this type, the IP packets destined for this destination will be forwarded to the next hop. It is the most common type of static routes.
- Unreachable route: route with ""**reject**" attribute". If a static route to a destination has the "**reject**" attribute, all the IP packets destined for this destination will be discarded, and the source hosts will be informed of the unreachability of the destination.
- Blackhole route: route with "**blackhole**" attribute. If a static route destined for a destination has the "**blackhole**" attribute, the outgoing interface of this route is the Null 0 interface regardless of the next hop address, and all the IP packets addressed to this destination will be dropped without notifying the source hosts.

The attributes "**reject**" and "**blackhole**" are usually used to limit the range of the destinations this router can reach, and help troubleshoot the network.

Default Route

A default route is a special route. You can manually configure a default route by using a static route. Some dynamic routing protocols, such as OSPF, can automatically generate a default route.

Simply put, a default route is a route used only when no matching entry is found in the routing table. That is, the default route is used only when there is no proper route. In a routing table, both the destination address and mask of the default route are 0.0.0.0. You can use the **display ip routing-table** command to view whether the default route has been set. If the destination address of a packet does not match any entry in the routing table, the router will select the default route for

the packet; in this case, if there is no default route, the packet will be discarded, and an Internet control message protocol (ICMP) packet will be returned to inform the source host that the destination host or network is unreachable.

Static Route Configuration

Configuration Prerequisites

Before configuring a static route, perform the following tasks:

- Configuring the physical parameters of the related interface
- Configuring the link layer attributes of the related interface
- Configuring an IP address for the related interface

Configuring a Static Route

Table 211 Configure a static route

Operation	Command	Description
Enter system view	**system-view**	-
Add a static route	**ip route-static** *ip-address* { *mask* | *mask-length* } { *interface-type interface-number* | *next-hop* } [**preference** *value*] [**reject** | **blackhole**]	Required By default, the system can obtain the route to the subnet directly connected to the router.
Delete all static routes	**delete static-routes all**	Optional This command deletes all static routes, including the default route.



- *If the destination IP address and the mask of a route are both 0.0.0.0, the route is the default route. Any packet for which the router fails to find a matching entry in the routing table will be forwarded through the default route.*
- *Do not configure the next hop address of a static route to the address of an interface on the local switch.*
- *The preference can be configured differently to implement flexible route management policy.*

Displaying and Maintaining the Routing Table

After the above configuration, use the **display** command in any view to display the static route configuration, so as to verify configuration result. You can use the **reset** command in user view to clear routing table statistics.

Table 212 Display the routing table

Operation	Command	Description
Display routing table summary	**display ip routing-table**	You can execute the **display** command in any view.
Display routing table details	**display ip routing-table verbose**	
Display the detailed information of a specific route	**display ip routing-table** *ip-address* [*mask*] [**longer-match**] [**verbose**]	
Display the routes in a specified address range	**display ip routing-table** *ip-address1 mask1 ip-address2 mask2* [**verbose**]	
Display the routes discovered by a specified protocol	**display ip routing-table protocol** *protocol* [**inactive** | **verbose**]	
Display the tree-structured routing table information	**display ip routing-table radix**	
Display the statistics of the routing table	**display ip routing-table statistics**	
Clear the statistics about a protocol in the routing table	**reset ip routing-table statistics protocol** { **all** | *protocol* }	Use the **reset** command in user view.

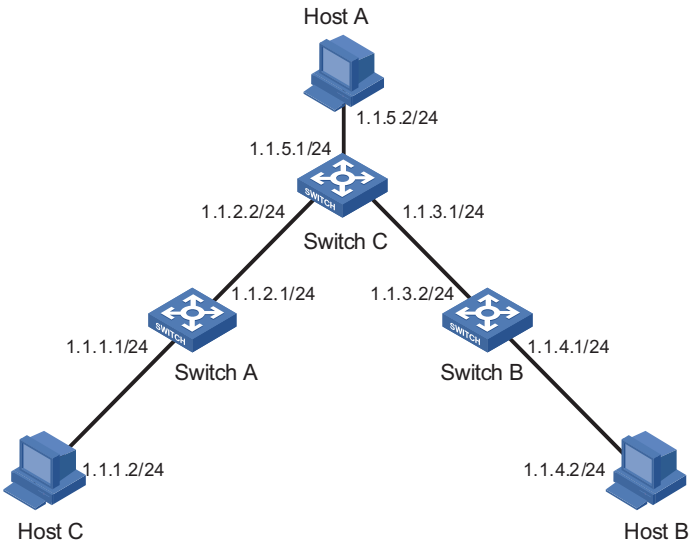
Static Route Configuration Example

Network requirements

As shown in Figure 69, it is required that all the hosts/Layer 3 switches in the figure can communicate with each other by configuring static routes.

Network diagram

Figure 69 Static route configuration



Configuration procedure

Before the following configuration, make sure that the Ethernet link layer works normally and the IP addresses of the VLAN interfaces have been configured correctly.

Configure static routes on Switch A.

```
<SwitchA>system-view
[SwitchA] ip route-static 1.1.3.0 255.255.255.0 1.1.2.2
[SwitchA] ip route-static 1.1.4.0 255.255.255.0 1.1.2.2
[SwitchA] ip route-static 1.1.5.0 255.255.255.0 1.1.2.2
```

Configure static routes on Switch B.

```
<SwitchB>system-view
[SwitchB] ip route-static 1.1.2.0 255.255.255.0 1.1.3.1
[SwitchB] ip route-static 1.1.5.0 255.255.255.0 1.1.3.1
[SwitchB] ip route-static 1.1.1.0 255.255.255.0 1.1.3.1
```

Configure static routes on Switch C.

```
<SwitchC>system-view
[SwitchC] ip route-static 1.1.1.0 255.255.255.0 1.1.2.1
[SwitchC] ip route-static 1.1.4.0 255.255.255.0 1.1.3.2
```

Configure the default gateway of Host A to 1.1.5.1. Detailed configuration procedure is omitted.

Configure the default gateway of Host B to 1.1.4.1. Detailed configuration procedure is omitted.

Configure the default gateway of Host C to 1.1.1.1. Detailed configuration procedure is omitted.

Now, all the hosts/switches in the figure can interconnect with each other.

Troubleshooting a Static Route

Symptom: The switch is not configured with a dynamic routing protocol. Both the physical status and the link layer protocol status of an interface are UP, but IP packets cannot be normally forwarded on the interface.

Solution: Perform the following procedure.

Use the **display ip routing-table protocol static** command to view whether the corresponding static route is correctly configured.

Use the **display ip routing-table** command to view whether the static route is valid.

33 RIP CONFIGURATION

RIP Overview

Routing information protocol (RIP) is a simple interior gateway protocol (IGP) suitable for small-sized networks.

Basic Concepts

RIP

RIP is a distance-vector (D-V) algorithm-based protocol. It exchanges routing information via UDP packets.

RIP uses hop count (also called routing cost) to measure the distance to a destination address. In RIP, the hop count from a router to its directly connected network is 0, and that to a network which can be reached through another router is 1, and so on. To restrict the time to converge, RIP prescribes that the cost is an integer ranging from 0 and 15. The hop count equal to or exceeding 16 is defined as infinite; that is, the destination network or host is unreachable.

To improve performance and avoid routing loop, RIP supports split horizon. Besides, RIP can import routes from other routing protocols.

RIP routing database

Each router running RIP manages a routing database, which contains routing entries to all the reachable destinations in the internetwork. Each routing entry contains the following information:

- Destination address: IP address of a host or network.
- Next hop address: IP address of an interface on the adjacent router that IP packets should pass through to reach the destination.
- Interface: Interface on this router, through which IP packets should be forwarded to reach the destination.
- Cost: Cost for the router to reach the destination.
- Routing time: Time elapsed after the routing entry is updated last time. This time is reset to 0 whenever the routing entry is updated.

RIP timers

As defined in RFC 1058, RIP is controlled by three timers: Period update, Timeout, and Garbage-collection.

- Period update timer: This timer is used to periodically trigger routing information update so that the router to send all RIP routes to all the neighbors.
- Timeout timer: If a RIP route is not updated (that is, the switch does not receive any routing update packet from the neighbor) within the timeout time of this timer, the route is considered unreachable.

- Garbage-collection timer: An unreachable route will be completely deleted from the routing table if no update packet for the route is received from the neighbor before this timer times out.

RIP Startup and Operation

The whole process of RIP startup and operation is as follows:

- Once RIP is enabled on a router, the router broadcasts or multicasts a request packet to its neighbors. Upon receiving the packet, each neighbor running RIP answers a response packet containing its routing table information.
- When this router receives a response packet, it modifies its local routing table and sends an update triggering packet to the neighbor. Upon receiving the update triggering packet, the neighbor sends the packet to all its neighbors. After a series of update triggering processes, each router can get and keep the updated routing information.
- By default, RIP sends its routing table to its neighbors every 30 seconds. Upon receiving the packets, the neighbors maintain their own routing tables and select optimal routes, and then advertise update information to their respective neighbors so as to make the updated routes known globally. Furthermore, RIP uses the timeout mechanism to handle the timeout routes so as to ensure real-time and valid routes.

RIP is commonly used by most IP router suppliers. It can be used in most campus networks and the regional networks that are simple and less dispersive. For larger and more complicated networks, RIP is not recommended.

Introduction to RIP Configuration Tasks

Table 213 RIP configuration tasks

Configuration Task		Description	Related section
Configuring Basic RIP Functions	Enabling RIP globally and on the interface of a specified network segment	Required	"Enabling RIP globally and on the interface of a specified network segment" on page 292
	Setting the RIP operating status on an interface	Optional	"Setting the RIP operating status on an interface" on page 292
	Specifying the RIP version on an interface	Optional	"Specifying the RIP version on an interface" on page 292

Table 213 RIP configuration tasks

Configuration Task		Description	Related section
Configuring RIP Route Control	Setting the additional routing metrics of an interface	Optional	"Setting the additional routing metrics of an interface" on page 293
	Configuring RIP route summary	Optional	"Configuring RIP route summary" on page 294
	Disabling the receiving of host routes	Optional	"Disabling the receiving of host routes" on page 294
	Configuring RIP to filter or advertise the received routes	Optional	"Configuring RIP to filter or advertise the received routes" on page 295
	Setting RIP preference	Optional	"Setting RIP preference" on page 295
	Enabling RIP traffic sharing across interfaces	Optional	"Enabling RIP traffic sharing across interfaces" on page 295
	Configuring RIP to import routes from another protocol	Optional	"Configuring RIP to redistribute routes from another protocol" on page 296
RIP Network Adjustment and Optimization	Configuring RIP timers	Optional	"Configuring RIP timers" on page 297
	Configuring split horizon	Optional	"Configuring split horizon" on page 297
	Configuring RIP-1 packet zero field check	Optional	"Configuring RIP-1 packet zero field check" on page 297
	Setting RIP-2 packet authentication mode	Optional	"Setting RIP-2 packet authentication mode" on page 297
	Configuring a RIP neighbor	Optional	"Configuring a RIP neighbor" on page 298

Basic RIP Configuration

Configuration Prerequisites

Before configuring basic RIP functions, perform the following tasks:

- Configuring the link layer protocol

- Configuring the network layer addresses of interfaces so that adjacent nodes are reachable to each other at the network layer

Configuring Basic RIP Functions

Enabling RIP globally and on the interface of a specified network segment

Table 214 Enable RIP globally and on the interface of a specified network segment

Operation	Command	Description
Enter system view	**system-view**	-
Enable RIP globally and enter RIP view	**rip**	-
Enable RIP on the interface of a specified network segment	**network** *network-address*	Required By default, RIP is disabled on any interface.



- *RIP can be enabled on an interface only after it has been enabled globally.*
- *RIP operates on the interface of a network segment only when it is enabled on the interface. When RIP is disabled on an interface, it does not operate on the interface, that is, it neither receives/sends routes on the interface nor forwards its interface route. Therefore, after RIP is enabled globally, you must also specify its operating network segments to enable it on the corresponding interfaces.*

Setting the RIP operating status on an interface

Table 215 Setting the RIP operating status on an interface

Operation	Command	Description
Enter system view	**system-view**	-
Enter interface view	**interface** *interface-type interface-number*	-
Enable the interface to receive RIP update packets	**rip input**	Optional By default, except for loopback interface, all interfaces are allowed to send and receive RIP packets.
Enable the interface to send RIP update packets	**rip output**	
Run RIP on the interface	**rip work**	

Specifying the RIP version on an interface

Table 216 Specify the RIP version on an interface

Operation	Command	Description
Enter system view	**system-view**	-
Enter interface view	**interface** *interface-type interface-number*	-

Table 216 Specify the RIP version on an interface

Operation	Command	Description
Specify RIP version on the interface	**rip version** { **1** | **2** [**broadcast** | **multicast**] }	Optional By default, the RIP version on an interface is RIP-1, and the interface can receive RIP-1 and RIP-2 broadcast packets but send only RIP-1 packets. When specifying the RIP version on an interface to RIP-2, you can also specify the mode (broadcast or multicast) to send RIP packets.

RIP Route Control

In actual implementation, it may be needed to control RIP routing information more accurately to accommodate complex network environments. By performing the configuration described in the following sections, you can:

- Control route selection by adjusting additional routing metrics on interfaces running RIP.
- Reduce the size of the routing table by setting route summary and disabling the receiving of host routes.
- Filter the received routes.
- Set the preference of RIP to change the preference order of routing protocols. This order makes sense when more than one route to the same destination is discovered by multiple routing protocols.
- Speed up packet forwarding by enabling RIP traffic sharing across interfaces
- Import external routes in an environment with multiple routing protocols and filter the advertised routes.

Configuration Prerequisites

Before configuring RIP route control, perform the following tasks:

- Configuring network layer addresses of interfaces so that adjacent nodes are reachable to each other at the network layer
- Configuring basic RIP functions

Configuring RIP Route Control

Setting the additional routing metrics of an interface

Additional routing metric is the routing metric (hop count) added to the original metrics of RIP routes on an interface. It does not change the metric value of a RIP route in the routing table, but will be added for incoming or outgoing RIP routes on the interface.

Table 217 Set additional routing metric

Operation	Command	Description
Enter system view	**system-view**	-
Enter interface view	**interface** *interface-type interface-number*	-

Table 217 Set additional routing metric

Operation	Command	Description
Set the additional routing metric to be added for incoming RIP routes on this interface	**rip metricin** *value*	Optional By default, the additional routing metric added for incoming routes on an interface is 0.
Set the additional routing metric to be added for outgoing RIP routes on this interface	**rip metricout** *value*	Optional By default, the additional routing metric added for outgoing routes on an interface is 1.

*The **rip metricout** command takes effect only on the RIP routes learnt by the router and the RIP routes generated by the router itself, but not on any route imported to RIP from other routing protocols.*

Configuring RIP route summary

Route summary means that different subnet routes in the same natural network segment can be aggregated into one route with a natural mask for transmission to another network segment. This function is used to reduce the routing traffic on the network as well as to reduce the size of the routing table.

Route summary does not work for RIP-1. RIP-2 supports route summary. When it is needed to advertise all subnet routes, you can disable the function for RIP-2.

Table 218 Configure RIP route summary

Operation	Command	Description
Enter system view	**system-view**	-
Enter RIP view	**rip**	-
Enable RIP-2 automatic route summary	**summary**	Optional By default, RIP-2 automatic route summary is enabled.

Disabling the receiving of host routes

In some special cases, the router can receive a lot of host routes from the same segment, and these routes are of little help in route addressing but consume a lot of network resources. After host route receiving is disabled, a router can refuse any incoming host routes.

Table 219 Disable the receiving of host route

Operation	Command	Description
Enter system view	**system-view**	-
Enter RIP view	**rip**	-
Disable the receiving of host routes	**undo host-route**	Optional By default, the router receives host routes.

Configuring RIP to filter or advertise the received routes

The route filtering function provided by a router enables you to configure inbound/outbound filter policy by specifying an ACL or address prefix list to make RIP filter incoming/outgoing routes. Besides, you can configure RIP to receive only the RIP packets from a specific neighbor.

Table 220 Configure RIP to filter incoming/outgoing routes

Operation	Command	Description
Enter system view	**system-view**	-
Enter RIP view	**rip**	-
Configure RIP to filter incoming routes	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* [**gateway** *ip-prefix-name*] | **gateway** *ip-prefix-name* } **import** [**interface** *interface-type interface-number*]	Required By default, RIP does not filter any incoming routes. The **gateway** keyword is used to filter the incoming routes advertised from a specified address.
	filter-policy route-policy *route-policy-name* **import**	
Configure RIP to filter outgoing routes	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol* [*process-id*] | **interface** *interface-type interface-number*]	Required By default, RIP does not filter any outgoing routes.
	filter-policy route-policy *route-policy-name* **export**	

- *The **filter-policy import** command filters the RIP routes received from neighbors, and the routes being filtered out will neither be added to the routing table nor be advertised to any neighbors.*
- *The **filter-policy export** command filters all the routes to be advertised, including the routes imported by using the **import-route** command as well as RIP routes learned from neighbors.*
- *The **filter-policy export** command without the routing-protocol argument filters all the routes to be advertised, including the routes imported by the **import-route** command.*

Setting RIP preference

Table 221 Set RIP preference

Operation	Command	Description
Enter system view	**system-view**	-
Enter RIP view	**rip**	-
Set the RIP preference	**preference** *value*	Optional The default RIP preference is 100.

Enabling RIP traffic sharing across interfaces

Table 222 Enable RIP traffic sharing across interfaces

Operation	Command	Description
Enter system view	**system-view**	-
Enter RIP view	**rip**	-

Table 222 Enable RIP traffic sharing across interfaces

Operation	Command	Description
Enable RIP traffic sharing across interfaces	**traffic-share-across-interface**	Optional By default, RIP traffic sharing across interfaces is disabled.

Configuring RIP to redistribute routes from another protocol

Table 223 Configure RIP to redistribute routes from another protocol

Operation	Command	Description
Enter system view	**system-view**	-
Enter RIP view	**rip**	-
Set the default cost for RIP to import routes from other protocols	**default cost** *value*	Optional When you use the **import-route** command without specifying the cost of imported routes, the default cost you set here will be used.
Configure RIP to redistribute routes from another protocol	**import-route** *protocol* [*process-id* | **allow-ibgp**] [**cost** *value* | **route-policy** *route-policy-name*]*	Optional



*The **allow-ibgp** keyword is used to redistribute iBGP routes. Because the AS-PATH attribute of redistributed iBGP routes is discarded, routing loops may occur. Therefore, use this keyword with caution.*

RIP Network Adjustment and Optimization

In some special network environments, some RIP features need to be configured and RIP network performance needs to be adjusted and optimized. By performing the configuration mentioned in this section, the following can be implemented:

- Changing the convergence speed of RIP network by adjusting RIP timers,
- Avoiding routing loop by configuring split horizon,
- Traffic sharing based on multiple equivalent routes,
- Packet validation in network environments with high security requirements, and
- Configuring RIP feature on an interface or link with special requirements.

Configuration Prerequisites

Before adjusting RIP, perform the following tasks:

- Configuring the network layer addresses of interfaces so that adjacent nodes are reachable to each other at the network layer
- Configuring basic RIP functions

Configuration Tasks

Configuring RIP timers

Table 224 Configure RIP timers

Operation	Command	Description
Enter system view	**system-view**	-
Enter RIP view	**rip**	-
Set the values of RIP timers	**timers** { **update** *update-timer* | **timeout** *timeout-timer* } *	Optional By default, Update timer value is 30 seconds and Timeout timer value is 180 seconds.

When configuring the values of RIP timers, you should take network performance into consideration and perform consistent configuration on all routers running RIP to avoid unnecessary network traffic and network route oscillation.

Configuring split horizon

Table 225 Configure split horizon

Operation	Command	Description
Enter system view	**system-view**	-
Enter interface view	**interface** *interface-type interface-number*	-
Enable split horizon	**rip split-horizon**	Optional By default, an interface uses split horizon to send RIP packets.

Split horizon cannot be disabled on a point-to-point link.

Configuring RIP-1 packet zero field check

Table 226 Configure RIP-1 packet zero field check

Operation	Command	Description
Enter system view	**system-view**	-
Enter RIP view	**rip**	-
Enable zero field check of RIP-1 packets	**checkzero**	Optional By default, zero field check is performed on RIP-1 packets.

Some fields in a RIP-1 packet must be 0, and they are known as zero fields. For RIP-1, zero field check is performed on incoming packets, those RIP-1 packets with nonzero value in a zero filed will not be processed further. As a RIP-2 packet has no zero fields, this configuration is invalid for RIP-2.

Setting RIP-2 packet authentication mode

RIP-2 supports two authentication modes, simple authentication and MD5 authentication.

Simple authentication cannot provide complete security, because the authentication keys sent along with packets are not unencrypted. Therefore, simple authentication cannot be applied where high security is required.

Table 227 Set RIP-2 packet authentication mode

Operation	Command	Description
Enter system view	**system-view**	-
Enter interface view	**interface** *interface-type interface-number*	-
Set RIP-2 packet authentication mode	**rip authentication-mode** { **simple** *password* | **md5** { **rfc2453** *key-string* | **rfc2082** *key-string key-id* } }	Required If you specify to use MD5 authentication, you must specify one of the following MD5 authentication types: rfc2453 (this type supports the packet format defined in RFC 2453) rfc2082 (this type supports the packet format defined in RFC 2082)

Configuring a RIP neighbor

Table 228 Configure a RIP neighbor

Operation	Command	Description
Enter system view	**system-view**	-
Enter RIP view	**rip**	-
Configure a RIP neighbor	**peer** *ip-address*	Required To make RIP works on a link that does not support broadcast/multicast packets, you must manually configure the RIP neighbor. Normally, RIP uses broadcast or multicast addresses to send packets.

Displaying and Maintaining RIP Configuration

After the above configuration, you can use the **display** command in any view to display the running status of RIP and verify the RIP configuration. You can use the **reset** command in RIP view to reset the system configuration related to RIP.

Table 229 Display and maintain RIP configuration

Operation	Command	Description
Display the current RIP running status and configuration information	**display rip**	You can execute the **display** command in any view.
Display RIP routing information	**display rip routing**	
Reset the system configuration related to RIP	**reset**	Use this command in RIP view.

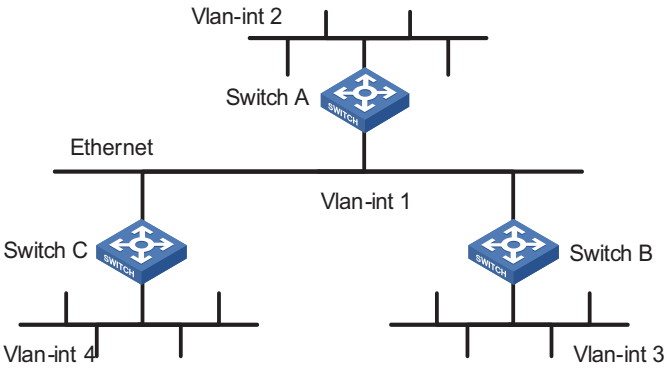
RIP Configuration Example

Network requirements

As shown in Figure 70, SwitchC is connected to subnet 117.102.0.0 through an Ethernet port. SwitchA and SwitchB are connected to networks 155.10.1.0 and 196.38.165.0 respectively through Ethernet ports. SwitchC, SwitchA and SwitchB are interconnected through Ethernet 110.11.2.0. It is required to configure RIP correctly to ensure the interworking between the networks connected to SwitchC, SwitchA and SwitchB.

Network diagram

Figure 70 RIP configuration



Device	Interface	IP address	Device	Interface	IP address
Switch A	Vlan-int1	110.11.2.1/24	Switch B	Vlan-int1	110.11.2.2/24
	Vlan-int2	155.10.1.1/24		Vlan-int3	196.38.165.1/24
Switch C	Vlan-int1	110.11.2.3/24			
	Vlan-int4	117.102.0.1/16			

Configuration procedure

Only the configuration related to RIP is listed below. Before the following configuration, make sure the Ethernet link layer works normally and the IP addresses of VLAN interfaces are configured correctly.

1 Configure SwitchA:

Configure RIP.

```
<SwitchA>system-view
[SwitchA] rip
[SwitchA-rip] network 110.11.2.0
[SwitchA-rip] network 155.10.1.0
```

2 Configure SwitchB:

Configure RIP.

```
<SwitchB>system-view
[SwitchB] rip
[SwitchB-rip] network 196.38.165.0
[SwitchB-rip] network 110.11.2.0
```

3 Configure SwitchC:

Configure RIP.

```
<SwitchC>system-view
[SwitchC] rip
[SwitchC-rip] network 117.102.0.0
[SwitchC-rip] network 110.11.2.0
```

Troubleshooting RIP Configuration

Symptom: The layer 3 switch cannot receive any RIP update packet when the physical connection between the switch and the peer routing device is normal.

Solution:

- Use the **display current-configuration configuration rip** command to verify RIP is enabled on the interface with the **network** command.
- Use the **display this** command in VLAN interface view to verify the **undo rip work** command was not executed on the interface connected to the peer.
- Use the **display this** command in VLAN interface view to verify the RIP packets sent by the two ends have the same format.

The peer routing device is configured to work in the multicast mode (for example, the **rip version 2 multicast** command is executed) but the multicast mode is not configured on the corresponding interface of this switch.

34 OSPF CONFIGURATION

OSPF Overview

Introduction to OSPF

Open shortest path first (OSPF) is a link state-based interior gateway protocol developed by IETF. At present, OSPF version 2 (RFC 2328) is used, which has the following features:

- High applicability: OSPF supports networks of various sizes and can support up to several hundred routers.
- Fast convergence: OSPF can transmit update packets immediately after the network topology changes so that the change can be synchronized in the autonomous system (AS).
- Loop-free: Since OSPF calculates routes with the shortest path tree algorithm according to the collected link states, it guarantees that no loop routes will be generated from the algorithm basis.
- Area partition: OSPF allows an autonomous system network to be divided into different areas for convenient management so that routing information transmitted between the areas is abstracted further, thereby reducing network bandwidth consumption.
- Equivalent route: OSPF supports multiple equivalent routes to the same destination.
- Routing hierarchy: OSPF has a four-level routing hierarchy. It prioritizes the routes as intra-area, inter-area, external type-1, and external type-2 routes.
- Authentication: OSPF supports interface-based packet authentication to guarantee the security of route calculation.
- Multicast transmission: OSPF supports transmitting protocol packets in multicast mode.

OSPF Route Calculation

Taking no account of area partition, the routing calculation process of the OSPF protocol is as follows:

- Each OSPF-capable router maintains a link state database (LSDB), which describes the topology of the whole AS. According to the network topology around itself, each router generates a link state advertisement (LSA). Routers on the network exchange LSAs with each other by transmitting protocol packets. Thus, each router receives the LSAs of other routers and all these LSAs form the LSDB of the router.
- An LSA describes the network topology around a router, whereas an LSDB describes the network topology of the whole network. Routers can easily transform the LSDB to a weighted directed map, which actually reflects the

topology of the whole network. Obviously, all routers get exactly the same map.

- A router uses the shortest path first (SPF) algorithm to calculate the shortest path tree with itself as the root. The tree shows the routes to the nodes in the autonomous system. External routes are leaf nodes, which are marked with the routers from which they are advertised to record information outside the AS. Obviously, the routing tables obtained by different routers are different.

Furthermore, to enable individual routers to broadcast their local status information (such as available interface information and reachable neighbor information) to the whole AS, routers in the AS should establish neighboring relationship among them. In this case, the route changes on any router will result in multiple transmissions, which are unnecessary and waste the precious bandwidth resources. To solve this problem, designated router (DR) and backup designated router (BDR) are defined in OSPF. For details about DR and BDR, see "DR and BDR" on page 304.

OSPF supports interface-based packet authentication to guarantee the security of route calculation. In addition, it transmits and receives packets in multicast (224.0.0.5 and 224.0.0.6).

Basic OSPF Concepts

Router ID

To run OSPF, a router must have a router ID. A router ID can be configured manually. If no router ID is configured, the system will automatically select an IP address from the IP addresses of the interfaces as the router ID. A router ID is selected in the following way: if loopback interface addresses are configured, the system chooses the latest configured IP address as the router ID; if no loopback interface is configured, the first configured IP address among the IP addresses of other interfaces will be the router ID.

DR and BDR

For details, see "DR and BDR" on page 304.

Area

If all the routers on an ever-growing huge network run OSPF, the large number of routers will result in an enormous LSDB, which will consume an enormous storage space, complicate the running of SPF algorithm, and increase CPU load. Furthermore, as a network grows larger, it is more potential to have changes in the network topology. Hence, the network will often be in "turbulence", and a great number of OSPF packets will be generated and transmitted in the network. This will lower the network bandwidth utilization. In addition, each change will cause all the routers on the network re-perform route calculation.

OSPF solves the above-mentioned problem by dividing an AS into multiple areas. Areas group routers logically. A router on the border of an area belongs to more than one area. A router connecting the backbone area to a non-backbone area is called an area border router (ABR). An ABR can connect to the backbone area physically or logically.

Area partition in OSPF reduces the number of LSAs in the network and enhances OSPF scalability. To further reduce routing table size and the number of LSAs in

some non-backbone areas on the edge of the AS, you can configure these areas as stub areas.

A stub area cannot import any external route. For this reason the concept NSSA area (not-so-stubby area) is introduced. In an NSSA area, type 7 LSAs are allowed to be propagated. A type 7 LSA is generated by an ASBR (autonomous system boundary router) in a NSSA area. A type 7 LSA reaching an ABR in the NSSA area is transformed into an AS-external LSA, which is then advertised to other areas.

Backbone area and virtual link

Backbone Area

With OSPF area partition, not all areas are equal. One of the areas is different from any other area. Its area ID is 0 and it is usually called the backbone area.

Virtual link

Since all areas must be connected to the backbone area, the concept virtual link is introduced to maintain logical connectivity between the backbone area and any other area physically separated from the backbone area.

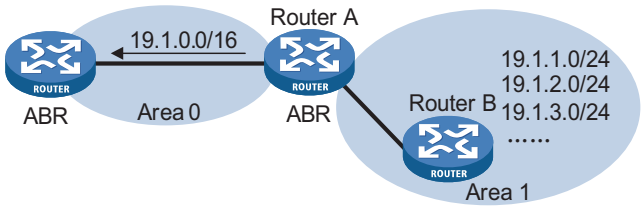
Route summary

After an AS is divided into different areas that are interconnected through OSPF ABRs, The routing information between areas can be reduced through route summary. This reduces the size of routing tables and improves the calculation speed of routers.

After an ABR in an area calculates the intra-area routes in the area, the ABR aggregates multiple OSPF routes into one LSA (based on the summary configuration) and sends the LSA outside the area.

For example, as shown in Figure 71, there are three intra-area routes in Area 1: 19.1.1.0/24, 19.1.2.0/24, and 19.1.3.0/24. If route summary is configured, the three routes are aggregated into one route 19.1.0.0/16, and only one corresponding LSA is generated on Router A into Area 0.

Figure 71 Area partition and route aggregation



OSPF Network Type

Four OSPF network types

OSPF divides networks into four types by link layer protocols:

- Broadcast: If Ethernet or FDDI is adopted, OSPF defaults the network type to broadcast. In a broadcast network, protocol packets are sent in multicast (224.0.0.5 and 224.0.0.6) by default.

- Non-broadcast multi-access (NBMA): If Frame Relay, ATM, or X.25 is adopted, OSPF defaults the network type to NBMA. In an NBMA network, protocol packets are sent in unicast.
- Point-to-multipoint (P2MP): OSPF will not default the network type of any link layer protocol to P2MP. A P2MP network must be compulsorily changed from another network type. The common practice is to change an NBMA network into a P2MP network. In a P2MP network, protocol packets are sent in multicast (224.0.0.5).
- Point-to-point (P2P): If PPP or HDLC is adopted, OSPF defaults the network type to P2P. In a P2P network, protocol packets are sent in multicast (224.0.0.5).

Principles for configuring an NBMA network

An NBMA network is a non-broadcast and multi-accessible network. ATM and frame relay networks are typical NBMA networks.

Some special configurations need to be done on an NBMA network. In an NBMA network, an OSPF router cannot discover an adjacent router by broadcasting Hello packets. Therefore, you must manually specify an IP address for the adjacent router and whether the adjacent router has the right to vote for a DR.

An NBMA network must be fully connected. That is, any two routers in the network must be directly reachable to each other through a virtual circuit. If two routers in the network are not directly reachable to each other, you must configure the corresponding interface type to P2MP. If a router in the network has only one peer, you can change the corresponding interface type to P2P.

The differences between NBMA and P2MP are as follows:

- An NBMA network is fully connected, non-broadcast, and multi-accessible, whereas a P2MP network is not necessarily fully connected.
- DR and BDR are required to be elected on an NBMA network but not on a P2MP network.
- NBMA is a default network type. A P2MP network, however, must be compulsorily changed from another network type. The more common practice is to change an NBMA network into a P2MP network.
- NBMA sends protocol packets in unicast and neighbors should be configured manually, while P2MP sends protocol packets in multicast.

DR and BDR

In a broadcast network or an NBMA network, routing information needs to be transmitted between any two routers. If there are n routers in the network, n x (n-1)/2 adjacencies need to be established. In this case, the route changes on any router will result in multiple transmissions, which waste bandwidth. To solve this problem, DR is defined in OSPF so that all routers send information to the DR only and the DR broadcasts the network link states in the network.

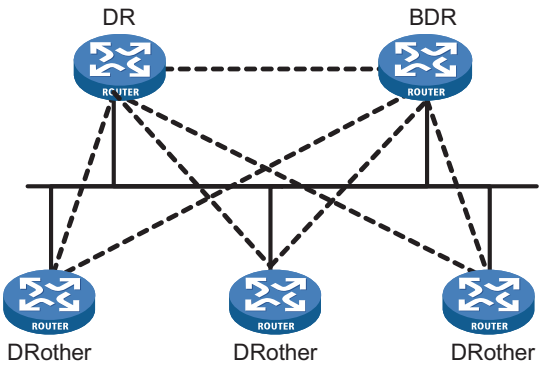
If the DR fails, a new DR must be elected and synchronized with the other routers on the network. The process takes quite a long time; in the process, route calculation is incorrect. To shorten the process, BDR is introduced in OSPF.

In fact, a BDR provides backup for a DR. DR and BDR are elected at the same time. Adjacencies are also established between the BDR and all the other routers on the segment, and routing information is also exchanged between them. Once the DR becomes invalid, the BDR becomes a DR. Since no re-election is needed and the adjacencies already exist, the switchover process is very short. Now, a new BDR should be elected. Although this election process will also take quite a long time, route calculation will not be affected.

Neither neighboring relationship is established nor routing information is exchanged between DR Others (routers other than DR and BDR). This reduces the number of adjacencies among routers on the broadcast or NBMA network.

As shown in Figure 72, the solid lines represent physical Ethernet connections and the dotted lines represent adjacencies established. The figure shows that, with the DR/BDR mechanism adopted, seven adjacencies suffice among the five routers.

Figure 72 DR and BDR



DR/BDR election

Instead of being manually configured, DR and BDR are elected by all the routers on the current network segment. The priority of a router interface determines the qualification of the interface in DR/BDR election. All the routers with DR priorities greater than 0 in the current network segment are eligible "candidates".

Hello packets serve as the "votes" in the election. Each router writes the DR it selects to the Hello packet and sends the packet to each router running OSPF in the network segment. If two routers on the same network segment declare themselves to be the DR, the one with the highest DR priority will be preferred. If their priorities are the same, the one with greater router ID will be preferred. A router whose DR priority is 0 can neither be elected as the DR nor be elected as the BDR.

Note the following points:

- DR election is required for broadcast or NBMA interfaces but is not required for P2P or P2MP interfaces.
- DR is based on the router interfaces in a certain segment. A router may be a DR on an interface and a BDR or DR Other on another interface.
- If a new router is added after DR and BDR election, the router does not become the DR immediately even if it has the highest DR priority.

- The DR on a network segment is not necessarily the router with the highest priority. Likewise, the BDR is not necessarily the router with the second-highest priority.

OSPF Packets

OSPF uses five types of packets:

Hello packet

Hello packets are most commonly used OSPF packets, which are periodically sent by a router to its neighbors. A Hello packet contains the values of some timers, the DR, the BDR and the known peers.

DD packet

When two routers synchronize their databases, they use database description (DD) packets to describe their own LSDBs, including the digest of each LSA. The digest refers to the HEAD of an LSA which uniquely identifies the LSA. This reduces the size of traffic transmitted between the routers because the HEAD of an LSA only occupies a small portion of the LSA. With the HEAD, the peer router can judge whether it has the LSA or not.

LSR packet

After exchanging DD packets, the two routers know which LSAs of the peer router are lacked in the local LSDB, and send link state request (LSR) packets requesting for the lacked LSAs to the peer. These LSR packets contain the digest of the needed LSAs.

LSU packet

Link state update (LSU) packets are used to transmit the needed LSAs to the peer router. An LSU packet is a collection of multiple LSAs (complete LSAs, not LSA digest).

LSAck packet

Link state acknowledgment (LSAck) packets are used to acknowledge received LSU packets. An LSAck contains the HEAD(s) of LSA(s) to be acknowledged (one LSAck packet can acknowledge multiple LSAs).

LSA Types

Five basic LSA types

As described in the preceding sections, LSAs are the primary source for OSPF to calculate and maintain routes. RFC 2328 defines five types of LSAs:

- Router-LSA: Type-1 LSAs, generated by every router to describe the router's link states and costs and advertised only in the area where the router resides.
- Network-LSA: Type-2 LSAs, generated by the DRs of broadcast or NBMA network to describe the link states of the current network segment and are advertised only in the area where the DRs reside.
- Summary-LSA: Type-3 and Type-4 LSAs, generated by ABRs and advertised in the areas associated with the LSAs. Each Summary-LSA describes a route to a destination in another area of the AS (also called inter-area route).Type-3 Summary-LSAs are for routes to networks (that is, their destinations are segments), while Type-4 Summary-LSAs are for routes to ASBRs.

- AS-external-LSA: Type-5 LSA, also called ASE LSA, generated by ASBRs to describe the routes to other ASs and advertised to the whole AS (excluding stub areas). The default AS route can also be described by AS-external-LSAs.

Type-7 LSAs

In RFC 1587 (OSPF NSSA Option), Type-7 LSA, a new LSA type, is added.

As described in RFC 1587, Type-7 LSAs and Type-5 LSAs mainly differ in the following two ways:

- Type-7 LSAs are generated and advertised in an NSSA, where Type-5 LSAs will not be generated or advertised.
- Type-7 LSAs can only be advertised in an NSSA area. When Type-7 LSAs reach an ABR, the ABR can convert part of the routing information carried in the Type-7 LSAs into Type-5 LSAs and advertise the Type-5 LSAs. Type-7 LSAs are not directly advertised to other areas (including the backbone area).

OSPF Features

Switch 7750 support the following OSPF features:

- Stub area: Stub area is defined to reduce the cost for the routers in the area to receive ASE routes.
- NSSA area: NSSA area is defined to remove the limit on the topology in a stub area.
- OSPF multi-process: Multiple OSPF processes can be run on a router.
- Sharing discovered routing information with other dynamic routing protocols: At present, OSPF supports importing the routes of other dynamic routing protocols (such as RIP), and static routes as OSPF external routes into the AS to which the router belongs. In addition, OSPF supports advertising the routing information it discovered to other routing protocols.
- Authentication key: OSPF supports the authentication of the packets between neighboring routers in the same area by using one of the two methods: plain text authentication key and MD5 authentication key.
- Flexible configuration of router interface parameters: For a router interface, you can configure the following OSPF parameters: output cost, Hello interval, interface transmission delay, route priority, dead time for a neighboring router, and packet authentication mode and authentication key.
- Virtual link: Virtual links can be configured.

Introduction to OSPF Configuration Tasks

Table 230 OSPF configuration tasks

Configuration Task	Description	Related section
Basic OSPF Configuration	Required	"Basic OSPF Configuration" on page 309
OSPF Area Attribute Configuration	Optional	"OSPF Area Attribute Configuration" on page 311

Table 230 OSPF configuration tasks

Configuration Task		Description	Related section
OSPF Network Type Configuration	Configuring the Network Type of an OSPF Interface	Optional	"Configuring the Network Type of an OSPF Interface" on page 312
	Setting an NBMA Neighbor	Optional	"Setting an NBMA Neighbor" on page 313
	Setting the DR Priority on an OSPF Interface	Optional	"Setting the DR Priority on an OSPF Interface" on page 313
OSPF Route Control	Configuring OSPF Route Summary	Optional	"Configuring OSPF Route Summary" on page 314
	Configuring OSPF to Filter Received Routes	Optional	"Configuring OSPF to Filter Received Routes" on page 314
	Configuring the Cost for Sending Packets on an OSPF Interface	Optional	"Configuring the Cost for Sending Packets on an OSPF Interface" on page 315
	Setting OSPF Route Priority	Optional	"Setting OSPF Route Priority" on page 315
	Configuring OSPF to Import External Routes	Optional	"Configuring OSPF Route Redistribution" on page 315

Table 230 OSPF configuration tasks

Configuration Task		Description	Related section
OSPF Network Adjustment and Optimization	Configuring OSPF Timers	Optional	"Configuring OSPF Timers" on page 317
	Configuring the LSA transmission delay	Optional	"Configuring the LSA transmission delay" on page 318
	Configuring the SPF Calculation Interval	Optional	"Configuring the SPF Calculation Interval" on page 318
	Disabling OSPF Packet Transmission on an Interface	Optional	"Disabling OSPF Packet Transmission on an Interface" on page 318
	Configuring OSPF Authentication	Optional	"Configuring OSPF Authentication" on page 319
	Configuring to Fill the MTU Field When an Interface Transmits DD Packets	Optional	"Configuring to Fill the MTU Field When an Interface Transmits DD Packets" on page 319
	Enabling OSPF Logging	Optional	"Enabling OSPF Logging" on page 320
	Configuring OSPF Network Management System (NMS)	Optional	"Configuring OSPF Network Management System (NMS)" on page 320

Basic OSPF Configuration

Before you can configure other OSPF features, you must first enable OSPF and specify the interface and area ID.

Configuration Prerequisites

Before configuring OSPF, perform the following tasks:

- Configuring the link layer protocol
- Configuring the network layer addresses of interfaces so that the adjacent nodes are reachable to each other at the network layer

Basic OSPF Configuration

Basic OSPF configuration includes:

- Configuring router ID

To ensure stable OSPF operation, you should determine the division of router IDs and manually configure them when implementing network planning. When you

configure router IDs manually, make sure each router ID is uniquely used by one router in the AS. A common practice is to set the router ID to the IP address of an interface on the router.

- Enabling OSPF

The Switch 7750 supports multiple OSPF processes. To enable multiple OSPF processes on a router, you need to specify different process IDs. OSPF process ID is only locally significant; it does not affect the packet exchange between an OSPF process and other routers. Therefore, packets can be exchanged between routers with different OSPF processes IDs.

- Configuring an area and the network segments in the area. You need to plan areas in an AS before performing the corresponding configurations on each router.

When configuring the routers in the same area, please note that most configurations should be uniformly made based on the area. Wrong configuration may disable information transmission between neighboring routers and even lead to congestion or self-loop of routing information.

Table 231 Basic OSPF configuration

Operation	Command	Description
Enter system view	**system-view**	-
Disable protocol multicast MAC address delivery	**undo protocol multicast-mac enable**	Optional
Configure the router ID	**router id** *router-id*	Optional If multiple OSPF processes run on a router, you are recommended to use the **router-id** keyword in the following command to specify different router IDs for different processes.
Enable OSPF and enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	-
Enter OSPF area view	**area** *area-id*	-
Configure the network segments in the area	**network** *address wildcard-mask*	Required By default, an interface does not belong to any area.



- *The **undo protocol multicast-mac enable** command must be configured if Layer 2/Layer 3 multicast function is enabled in the system.*
- *In router ID selection, the priorities of the router IDs configured with the **ospf** [process-id [**router-id** router-id]] command, the **router id** command, and the priorities of the router IDs automatically selected are in a descending order.*
- *Router IDs can be re-selected. A re-selected router ID takes effect only after the OSPF process is restarted.*
- *The **ospf** [process-id [**router-id** router-id]] command is recommended for configuring router IDs manually.*

- *The ID of an OSPF process is unique.*
- *One segment can belong to only one area and you must specify each OSPF interface to belong to a particular area.*

OSPF Area Attribute Configuration

Area partition in OSPF reduces the number of LSAs in the network and enhances OSPF scalability. To further reduce routing table size and the number of LSAs in some non-backbone areas on the edge of the AS, you can configure these areas as stub areas.

A stub area cannot import any external route. For this reason the concept of NSSA area is introduced. Type7 LSAs can be advertised in an NSSA area. Type7 LSAs are generated by ASBRs of the NSSA area, and will be transformed into AS-external LSAs whey reaching ABRs in the NSSA area, which will then be advertised to other areas.

After area partition, the OSPF route updates between non-backbone areas are exchanged by way of the backbone area. Therefore, OSPF requires that all the non-backbone areas should keep connectivity with the backbone area and the backbone area must keep connectivity in itself.

If the physical connectivity cannot be ensured due to various restrictions, you can configure OSPF virtual links to satisfy this requirement.

Configuration Prerequisites

Before configuring OSPF area attributes, perform the following tasks:

- Configuring the network layer addresses of interfaces so that the adjacent nodes are reachable to each other at the network layer
- Performing basic OSPF configuration

Configuring OSPF Area Attributes

Table 232 Configure OSPF area attributes

Operation	Command	Description
Enter system view	**system-view**	-
Enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	-
Enter OSPF area view	**area** *area-id*	-
Configure the current area to be a stub area	**stub** [**no-summary**]	Optional By default, no area is configured as a stub area.
Configure an area to be an NSSA area	**nssa** [**default-route-advertise** | **no-import-route** | **no-summary**]*	Optional By default, no area is configured as an NSSA area.
Configure the cost of the default route transmitted by OSPF to a stub or NSSA area	**default-cost** *cost*	Optional This can be configured on an ABR only. By default, the cost of the default route to a stub or NSSA area is 1.

Table 232 Configure OSPF area attributes

Operation	Command	Description
Create and configure a virtual link	**vlink-peer** *router-id* [**hello** *seconds* | **retransmit** *seconds* | **trans-delay** *seconds* | **dead** *seconds* | **simple** *password* | **md5** *keyid key*]*	Optional For a virtual link to take effect, you need to use this command at both ends of the virtual link and ensure consistent configurations of the **hello**, **dead**, and other parameters at both ends.

- *You must use the **stub** command on all the routers connected to a stub area to configure the area with the stub attribute.*
- *You must use the **nssa** command on all the routers connected to an NSSA area to configure the area with the NSSA attribute.*

OSPF Network Type Configuration

OSPF divides networks into four types by link layer protocol. See "OSPF Network Type" on page 303. An NBMA network must be fully connected. That is, any two routers in the network must be directly reachable to each other through a virtual circuit. However, in many cases, this cannot be implemented and you need to use a command to change the network type forcibly.

Configure the interface type as P2MP if not all the routers are directly accessible on an NBMA network. Change the interface type to P2P if the router has only one peer on the NBMA network.

In addition, when configuring a broadcast network or NBMA network, you can also specify DR priority for each interface to control the DR/BDR selection in the network. Thus, the router with higher performance and reliability can be selected as a DR or BDR.

Configuration Prerequisites

Before configuring the network type of an OSPF interface, perform the following tasks:

- Configuring the network layer address of the interface so that the adjacent node is reachable at network layer
- Performing basic OSPF configuration

Configuring the Network Type of an OSPF Interface

Table 233 Configure the network type of an OSPF interface

Operation	Command	Description
Enter system view	**system-view**	-
Enter interface view	**interface** *interface-type interface-number*	-
Configure the network type of the OSPF interface	**ospf network-type** { **broadcast** | **nbma** | **p2mp** | **p2p** }	Optional By default, the network type of an interface depends on the physical interface.

- *After an interface has been configured with a new network type, the original network type of the interface is removed automatically.*
- *Note that, neighboring relationship can be established between two interfaces configured as broadcast, NBMA, or P2MP only if the interfaces are on the same network segment.*

Setting an NBMA Neighbor

Some special configurations need to be done on an NBMA network. Since an NBMA interface cannot discover the adjacent router by broadcasting Hello packets, you must manually specify the IP address of the adjacent router for the interface and whether the adjacent router has the right to vote.

Table 234 Set NBMA neighbor

Operation	Command	Description
Enter system view	**system-view**	-
Enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	Required
Set an NBMA neighbor	**peer** *ip-address* [**dr-priority** *dr-priority-value*]	Required By default, the priority for the neighbor of an NBMA interface is 1.

Setting the DR Priority on an OSPF Interface

You can control the DR/BDR election on a broadcast or NBMA network by configuring the DR priorities of interfaces.

Table 235 Set the DR priority on an OSPF interface

Operation	Command	Description
Enter system view	**system-view**	-
Enter interface view	**interface** *interface-type interface-number*	Required
Set the DR priority on the OSPF interface	**ospf dr-priority** *priority*	Optional The default DR priority is 1.

*The DR priorities configured by the **ospf dr-priority** command and the **peer** command have different purpose*

- *The priority set with the **ospf dr-priority** command is used for actual DR election.*
- *The priority set with the **peer** command is used to indicate if a neighbor has the right to vote. If you specify the priority to 0 when configuring a neighbor, the local router will believe that the neighbor has no right to vote and sends no Hello packet to it. This configuration can reduce the number of Hello packets on the network during the election of DR and BDR. However, if the local router is already a DR or BDR, it will send Hello packets to the neighbor whose DR priority is 0 to establish the neighboring relationship.*

OSPF Route Control

Perform the following configurations to control the advertisement and reception of the routing information discovered by OSPF and import routing information discovered by other protocols.

Configuration Prerequisites

Before configuring OSPF route control, perform the following tasks:

- Configuring the network layer addresses of interfaces so that the adjacent nodes are reachable to each other at the network layer
- Completing basic OSPF configuration
- Configuring filter list to filter routing information

Configuring OSPF Route Summary

The configuration of OSPF route summary includes:

- Configuring ABR route summary,
- Configuring ASBR route summary for imported routes.

Table 236 Configure ABR route summary

Operation	Command	Description
Enter system view	**system-view**	-
Enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	-
Enter area view	**area** *area-id*	-
Enable ABR route summary	**abr-summary** *ip-address mask* [**advertise** | **not-advertise**]	Required This command takes effect only when it is configured on an ABR. By default, this function is disabled on an ABR.

Table 237 Configure ASBR route summary

Operation	Command	Description
Enter system view	**system-view**	-
Enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	-
Enable ASBR route summary	**asbr-summary** *ip-address mask* [**not-advertise** | **tag** *value*]	Required This command takes effect only when it is configured on an ASBR. By default, summary of imported routes is disabled.

Configuring OSPF to Filter Received Routes

Table 238 Configure OSPF to filter received routes

Operation	Command	Description
Enter system view	**system-view**	-
Enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	-
Configure to filter the received routes	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* | **gateway** *ip-prefix-name* } **import**	Required By default, OSPF does not filter received routing information.

OSPF is a dynamic routing protocol based on link state, with routing information hidden in LSAs. Therefore, OSPF cannot filter any advertised or received LSA. In

fact, the filter-policy import command filters the routes calculated by OSPF; only the routes passing the filter can be added to the routing table.

Configuring the Cost for Sending Packets on an OSPF Interface

Table 239 Configure the cost for sending packets on an OSPF interface

Operation	Command	Description
Enter system view	**system-view**	-
Enter interface view	**interface** *interface-type interface-number*	-
Configure the cost for sending packets on an OSPF interface	**ospf cost** *value*	Optional By default, OSPF calculates the cost for sending packets on an interface according to the current baud rate on the interface. For a VLAN interface on the switch, this value is fixed at 1.

Setting OSPF Route Priority

Since multiple dynamic routing protocols may be running on one router, the problem of route sharing and selection between various routing protocols arises. The system sets a priority for each routing protocol (which you can change manually), and when more than one route to the same destination is discovered by different protocols, the route with the highest priority will take preference over other routes.

Table 240 Set OSPF route priority

Operation	Command	Description
Enter system view	**system-view**	-
Enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	-
Set OSPF route priority	**preference** [**ase**] *value*	Optional By default, the OSPF route priority is 10 and the priority of OSPF ASE is 150.

Configuring OSPF Route Redistribution

Table 241 Configure OSPF route redistribution

Operation	Command	Description
Enter system view	**system-view**	-
Enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	-
Enable OSPF to redistribute routes from another routing protocol	**import-route** *protocol* [*process-id* | **allow-ibgp**] [**cost** *value* | **type** *value* | **tag** *value* | **route-policy** *route-policy-name*]*	Required By default, OSPF does not import the routing information of other protocols.
Enable OSPF to filter advertised routes	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol*]	Optional By default, OSPF does not filter advertised routes.

Table 241 Configure OSPF route redistribution

Operation	Command	Description
Enable OSPF to redistribute a default route	**default-route-advertise** [**always** | **cost** *value* | **type** *type-value* | **route-policy** *route-policy-name*]*	Optional By default, OSPF does not redistribute the default route.
Configure the default cost for redistributed routes	**default cost** *value*	Optional By default, the cost for OSPF to import external routes is 1.
Configure the default maximum number of external routes imported by OSPF per unit time	**default limit** *routes*	Optional By default, a maximum of 1000 routes can be imported.
Configure the default tag for redistributed routes	**default tag** *tag*	Optional The default tag is 1 by default.
Configure the default type for redistributed routes	**default type** { **1** | **2** }	Optional By default, the type of redistributed routes is Type-2.

- *The **import-route** command cannot import a default route. To import the default route, you must use the **default-route-advertise** command.*
- *The filtering of advertised routes by OSPF means that OSPF only converts the external routes meeting the filter criteria into Type-5 or Type-7 LSAs and advertises them.*
- *When enabling OSPF to import external routes, you can also configure the defaults of some additional parameters, such as cost, number of routes, tag, and type. A route tag can be used to identify protocol-related information.*
- *The **allow-ibgp** keyword is used to redistribute iBGP routes. Because the AS-PATH attribute of redistributed iBGP routes is discarded, routing loops may occur. Therefore, use this keyword with caution.*

OSPF Network Adjustment and Optimization

You can adjust and optimize an OSPF network in the following aspects:

- By changing the OSPF packet timers, you can adjust the convergence speed of the OSPF network and the network load brought by OSPF packets. On some low-speed links, you need to consider the delay experienced when the interfaces transmit LSAs.
- By Adjusting SPF calculation interval, you can mitigate resource consumption caused by frequent network changes.
- In a network with high security requirements, you can enable OSPF authentication to enhance OSPF network security.
- In addition, OSPF supports network management. You can configure the binding of the OSPF MIB with an OSPF process and configure the Trap message transmission and logging functions.

Configuration Prerequisites

Before adjusting and optimizing an OSPF network, perform the following tasks:

- Configuring the network layer addresses of interfaces so that the adjacent nodes are reachable to each other at the network layer
- Configuring basic OSPF functions

Configuring OSPF Timers

The Hello intervals for OSPF neighbors must be consistent. The value of Hello interval is in inverse proportion to route convergence speed and network load.

The dead time on an interface must be at least four times of the Hello interval on the same interface.

After a router sends an LSA to a neighbor, it waits for an acknowledgement packet from the neighbor. If the router receives no acknowledgement packet from the neighbor within the retransmission interval, it retransmits the LSA to the neighbor.

Table 242 Configure OSPF timers

Operation	Command	Description
Enter system view	**system-view**	-
Enter interface view	**interface** *interface-type interface-number*	-
Set the hello interval on the interface	**ospf timer hello** *seconds*	Optional By default, **p2p** and **broadcast** interfaces send Hello packets every 10 seconds; while **p2mp** and **NBMA** interfaces send Hello packets every 30 seconds.
Set the poll interval on the NBMA interface	**ospf timer poll** *seconds*	Optional By default, poll packets are sent every 120 seconds.
Set the dead time of the neighboring router on the interface	**ospf timer dead** *seconds*	Optional By default, the dead time for the OSPF neighboring router on a **p2p** or **broadcast** interface is 40 seconds and that for the OSPF neighboring router on a **p2mp** or **NBMA** interface is 120 seconds.
Set the interval at which the router retransmits an LSA to the neighboring router on the interface	**ospf timer retransmit** *interval*	Optional By default, this interval is five seconds.



- *Default Hello and Dead timer values will be restored once the network type is changed.*
- *Do not set an LSA retransmission interval that is too short. Otherwise, unnecessary retransmission will occur. LSA retransmission interval must be greater than the round trip time of a packet between two routers.*

Configuring the LSA transmission delay

Table 243 Configure the LSA transmission delay

Operation	Command	Description
Enter system view	**system-view**	-
Enter interface view	**interface** *interface-type interface-number*	-
Configure the LSA transmission delay	**ospf trans-delay** *seconds*	Optional By default, the LSA transmission delay is one second.



The transmission of OSPF packets on a link also takes time. Therefore, a transmission delay should be added to the aging time of LSAs before the LSAs are transmitted. For a low-speed link, pay close attention on this configuration.

Configuring the SPF Calculation Interval

Whenever the LSDB of OSPF is changed, the shortest paths need to be recalculated. When the network changes frequently, calculating the shortest paths immediately after LSDB changes will consume enormous resources and affect the operation efficiency of the router. By adjusting the minimum SPF calculation interval, you can lighten the negative affection caused by frequent network changes.

Table 244 Set the SPF calculation interval

Operation	Command	Description
Enter system view	**system-view**	-
Enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	-
Set the SPF calculation interval	**spf-schedule-interval** *interval*	Optional By default, the SPF calculation interval is five seconds.

Disabling OSPF Packet Transmission on an Interface

To prevent OSPF routing information from being acquired by the routers on a certain network, use the **silent-interface** command to disable OSPF packet transmission on the corresponding interface.

Table 245 Disable OSPF packet transmission through an interface

Operation	Command	Description
Enter system view	**system-view**	-
Enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	-
Disable OSPF packet transmission on a specified interface	**silent-interface** *silent-interface-type silent-interface-number*	Required By default, all the interfaces are allowed to transmit OSPF packets.



- *On the same interface, you can disable multiple OSPF processes from transmitting OSPF packets. The **silent-interface** command, however, only applies to the OSPF interface where the specified process has been enabled, without affecting the interface for any other process.*

- *After an OSPF interface is set to be in silent status, the interface can still advertise its direct route. However, the Hello packets from the interface will be blocked, and no neighboring relationship can be established on the interface. This enhances OSPF networking adaptability, thus reducing the consumption of system resources.*

Configuring OSPF Authentication

Table 246 Configure OSPF authentication

Operation	Command	Description
Enter system view	**system-view**	-
Enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	-
Enter OSPF area view	**area** *area-id*	-
Configure the authentication mode of the OSPF area	**authentication-mode** { **simple** | **md5** }	Required By default, no authentication mode is configured for an area.
Return to OSPF view	**quit**	-
Return to system view	**quit**	-
Enter interface view	**interface** *interface-type interface-number*	-
Configure the authentication mode of the OSPF interface	**ospf authentication-mode** { **simple** *password* | **md5** *key-id key* }	Required By default, OSPF packets are not authenticated on an interface.

- *OSPF supports packet authentication and receives only those packets that are successfully authenticated. If packet authentication fails, no neighboring relationship will be established.*
- *The authentication modes for all routers in an area must be consistent. The authentication passwords for all routers on a network segment must also be consistent.*

Configuring to Fill the MTU Field When an Interface Transmits DD Packets

By default, an interface uses value 0 instead of its actual MTU value when transmitting DD packets. After the following configuration, the actual MTU value of the interface is filled in the Interface MTU field of the DD packets.

Table 247 Configure to fill the MTU field when an interface transmits DD packets

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet interface view	**interface** *interface-type interface-number*	-
Enable the interface to fill in the MTU field when transmitting DD packets	**ospf mtu-enable**	Required By default, the MTU value is 0 when an interface transmits DD packets. That is, the actual MTU value of the interface is not filled in.

Enabling OSPF Logging

Table 248 Enable OSPF logging

Operation	Command	Description
Enter system view	**system-view**	-
Enter OSPF view	**ospf** [*process-id* [**router-id** *router-id*]]	-
Enable the logging of neighbor status changes	**log-peer-change**	Optional Log neighbor status changes.

Configuring OSPF Network Management System (NMS)

Table 249 Configure OSPF MIB binding

Operation	Command	Description
Enter system view	**system-view**	-
Configure OSPF MIB binding	**ospf mib-binding** *process-id*	Optional By default, MIB is bound to the first enabled OSPF process. When multiple OSPF processes are enabled, you can configure to which OSPF process the MIB is bound.
Enable OSPF Trap	**snmp-agent trap enable ospf** [*process-id*] [**ifauthfail** | **ifcfgerror** | **ifrxbadpkt** | **ifstatechange** | **iftxretransmit** | **lsdbapproachoverflow** | **lsdboverflow** | **maxagelsa** | **nbrstatechange** | **originatelsa** | **vifauthfail** | **vifcfgerror** | **virifrxbadpkt** | **virifstatechange** | **viriftxretransmit** | **virnbrstatechange**]*	Optional You can configure OSPF to send diversified SNMP TRAP messages and specify a certain OSPF process to send SNMP TRAP messages by process ID.

Displaying OSPF Configuration

After the above configuration, you can use the **display** command in any view to display and verify the OSPF configuration.

You can use the **reset** command in user view to reset the OSPF counter or connection.

Table 250 Display configuration

Operation	Command	Description
Display brief information about one or all OSPF processes	**display ospf** [*process-id*] **brief**	You can execute the **display** command in any view.
Display OSPF statistics	**display ospf** [*process-id*] **cumulative**	
Display OSPF LSDB information	**display ospf** [*process-id*] [*area-id*] **lsdb** [**brief** | [**asbr** | **ase** | **network** | **nssa** | **router** | **summary** [*ip-address* **| verbose**]] [**originate-router** *ip-address* | **self-originate**]]	
Display OSPF peer information	**display ospf** [*process-id*] **peer** [**brief** | **statistics**]	
Display OSPF next hop information	**display ospf** [*process-id*] **nexthop**	
Display OSPF routing table	**display ospf** [*process-id*] **routing**	
Display OSPF virtual links	**display ospf** [*process-id*] **vlink**	
Display OSPF request list	**display ospf** [*process-id*] **request-queue**	
Display OSPF retransmission list	**display ospf** [*process-id*] **retrans-queue**	
Display the information about OSPF ABR and ASBR	**display ospf** [*process-id*] **abr-asbr**	
Display OSPF interface information	**display ospf** [*process-id*] **interface** [**verbose** | *interface-type interface-number* [**verbose**]]	
Display OSPF errors	**display ospf** [*process-id*] **error**	
Display OSPF ASBR summary information	**display ospf** [*process-id*] **asbr-summary** [*ip-address mask*]	
Reset one or all OSPF processes	**reset ospf** [**statistics**] { **all** | *process-id* }	Use the **reset** command in user view.

OSPF Configuration Example

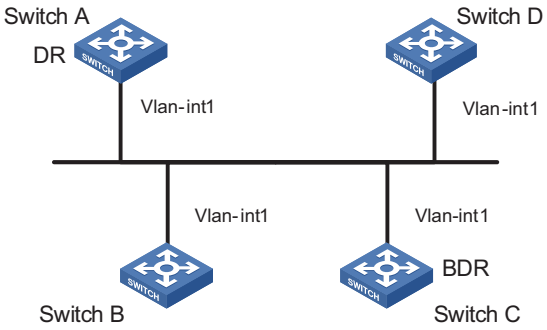
Configuring DR Election Based on OSPF Priority

Network requirements

Four Switch 7750, SwitchA, SwitchB, SwitchC, and SwitchD, which run OSPF, are on the same segment, as shown in Figure 73. Perform proper configurations to make SwitchA and SwitchC become DR and BDR respectively. Set the priority of SwitchA to 100 (the highest on the network) so that SwitchA is elected as the DR. Set the priority of SwitchC to 2 (the second highest priority) so that SwitchC is elected as the BDR. Set the priority of SwitchB to 0 so that SwitchB cannot be elected as the DR. No priority is set for SwitchD so it has a default priority of 1.

Network diagram

Figure 73 DR election based on OSPF priority



Device	Interface	IP address	Router ID	Interface DR priority
Switch A	Vlan-int1	196.1.1.1/24	1.1.1.1	100
Switch B	Vlan-int1	196.1.1.2/24	2.2.2.2	0
Switch C	Vlan-int1	196.1.1.3/24	3.3.3.3	2
Switch D	Vlan-int1	196.1.1.4/24	4.4.4.4	1

Configuration procedure

Configure SwitchA.

```
<SwitchA> system-view
[SwitchA] interface Vlan-interface 1
[SwitchA-Vlan-interface1] ip address 196.1.1.1 255.255.255.0
[SwitchA-Vlan-interface1] ospf dr-priority 100
[SwitchA] router id 1.1.1.1
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 196.1.1.0 0.0.0.255
```

Configure SwitchB.

```
<SwitchB> system-view
[SwitchB] interface Vlan-interface 1
[SwitchB-Vlan-interface1] ip address 196.1.1.2 255.255.255.0
[SwitchB-Vlan-interface1] ospf dr-priority 0
[SwitchB] router id 2.2.2.2
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 196.1.1.0 0.0.0.255
```

Configure SwitchC.

```
<SwitchC> system-view
[SwitchC] interface Vlan-interface 1
[SwitchC-Vlan-interface1] ip address 196.1.1.3 255.255.255.0
[SwitchC-Vlan-interface1] ospf dr-priority 2
[SwitchC] router id 3.3.3.3
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 196.1.1.0 0.0.0.255
```

Configure SwitchD.

```
<SwitchD> system-view
[SwitchD] interface Vlan-interface 1
[SwitchD-Vlan-interface1] ip address 196.1.1.4 255.255.255.0
[SwitchD] router id 4.4.4.4
[SwitchD] ospf
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 196.1.1.0 0.0.0.255
```

On SwitchA, run the **display ospf peer** command to display its OSPF peers. Note that SwitchA has three peers.

The state of each peer is full, which means that adjacency is established between SwitchA and each peer. SwitchA and SwitchC must establish adjacencies with all the switches on the network so that they can serve as the DR and BDR respectively on the network. SwitchA is DR, while SwitchC is BDR on the network. All the other neighbors are DR others (This means that they are neither DRs nor BDRs).

Change the priority of SwitchB to 200.

```
<SwitchB> system-view
[SwitchB] interface Vlan-interface 1
[SwitchB-Vlan-interface1] ospf dr-priority 200
```

On SwitchA, run the **display ospf peer** command to display its OSPF peers. Note that the priority of SwitchB has been changed to 200, but it is still not the DR.

The DR is changed only when the current DR turn offline. Shut down SwitchA, and run the **display ospf peer** command on SwitchD to display its peers. Note that the original BDR (SwitchC) becomes the DR and SwitchB becomes BDR now.

If all Ethernet Switches on the network are removed from and then added to the network again, SwitchB will be elected as the DR (with a priority of 200), and SwitchA will be the BDR (with a priority of 100). Shutting down and restarting all of the switches will bring about a new round of DR/BDR selection.

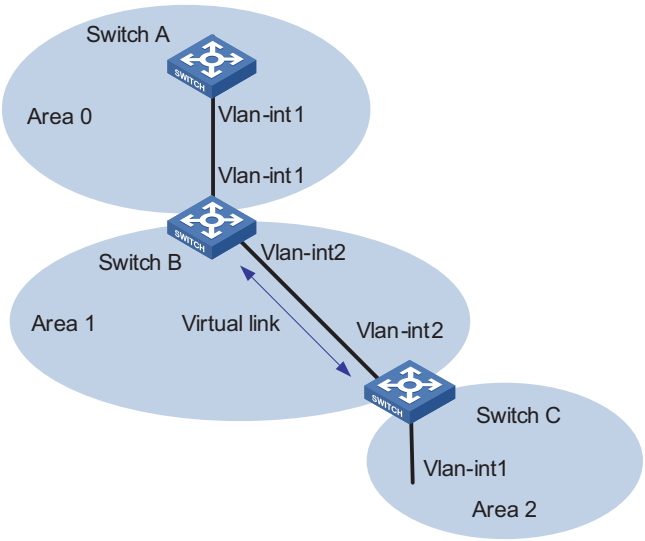
Configuring OSPF Virtual Link

Network requirements

As shown in Figure 74, Area 2 and Area 0 are not directly interconnected. It is required to use Area 1 as a transition area for interconnecting Area 2 and Area 0. Correctly configure a virtual link between SwitchB and SwitchC in Area 1.

Network diagram

Figure 74 OSPF virtual link configuration



Device	Interface	IP address	Router ID
Switch A	Vlan-int1	196.1.1.1/24	1.1.1.1
Switch B	Vlan-int1	196.1.1.2/24	2.2.2.2
	Vlan-int2	197.1.1.2/24	
Switch C	Vlan-int1	152.1.1.1/24	3.3.3.3
	Vlan-int2	197.1.1.1/24	

Configuration procedure

Configure SwitchA.

```
<SwitchA> system-view
[SwitchA] interface Vlan-interface 1
[SwitchA-Vlan-interface1] ip address 196.1.1.1 255.255.255.0
[SwitchA-Vlan-interface1] quit
[SwitchA] router id 1.1.1.1
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 196.1.1.0 0.0.0.255
```

Configure SwitchB.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 196.1.1.2 255.255.255.0
[SwitchB-Vlan-interface1] quit
[SwitchB] interface vlan-interface 2
[SwitchB-Vlan-interface2] ip address 197.1.1.2 255.255.255.0
[SwitchB] router id 2.2.2.2
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 196.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] area 1
```

```
[SwitchB-ospf-1-area-0.0.0.1] network 197.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.1] vlink-peer 3.3.3.3
```

Configure SwitchC.

```
<SwitchC> system-view
[SwitchC] interface Vlan-interface 1
[SwitchC-Vlan-interface1] ip address 152.1.1.1 255.255.255.0
[SwitchC-Vlan-interface1] quit
[SwitchC] interface Vlan-interface 2
[SwitchC-Vlan-interface2] ip address 197.1.1.1 255.255.255.0
[SwitchC-Vlan-interface2] quit
[SwitchC] router id 3.3.3.3
[SwitchC] ospf
[SwitchC-ospf-1] area 1
[SwitchC-ospf-1-area-0.0.0.1] network 197.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.1] quit
[SwitchC-ospf-1-area-0.0.0.1] vlink-peer 2.2.2.2
[SwitchC-ospf-1] area 2
[SwitchC-ospf-1-area-0.0.0.2] network 152.1.1.0 0.0.0.255
```

Troubleshooting OSPF Configuration

Symptom 1: OSPF has been configured in accordance with the above-mentioned steps, but OSPF does not run normally on the switch.

Solution: Perform the following procedure.

Local fault removal: Firstly, check whether the protocol works normally between two directly connected routers. The normal sign is that the peer state machine between the two routers reaches the FULL state. Note: On a broadcast or NBMA network, if the interfaces between two routers are in DROther state, the peer state machine between the two routers are in 2-way state, instead of FULL state. The peer state machine between DR/BDR and all the other routers is in FULL state.

- Use the **display ospf peer** command to view peers.
- Use the **display ospf interface** command to view the OSPF information on an interface.
- Check whether the physical connection is correct and the lower layer protocol operates normally. You can use the **ping** command to test. If the local router cannot ping through the peer router, it indicates that faults exist on the physical link and the lower level protocol.
- If the physical connection and the lower layer protocol are normal, check the OSPF parameters configured on the interface. Verify that these parameter configurations are consistent with those on the peer interface. The area IDs must be the same, and the network segments and the masks must also be consistent (**p2p** or virtually linked segments can have different segments and masks).
- Ensure that the dead timer value is at least four times of the hello timer value on the same interface.
- If the network type is NBMA, you must use the **peer ip-address** command to manually specify a peer.

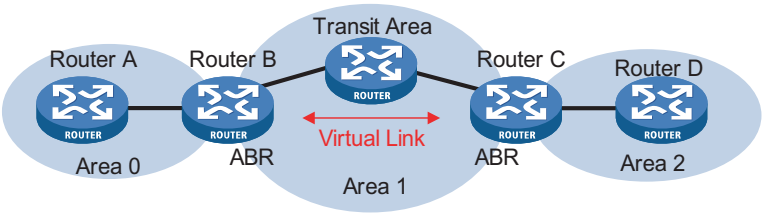
- If the network type is broadcast or NBMA, ensure that there is at least one interface with a priority greater than zero.
- If an area is set to a stub area, ensure that the area is set to a stub area for all the routers connected to this area.
- Ensure that the interface types of two neighboring routers are consistent.
- If two or more areas are configured, ensure that at least one area is configured as the backbone area; that is, the area ID of an area is 0.
- Ensure that the backbone area is connected to all the other areas.
- Ensure that no virtual link passes through a stub area.

Global fault removal: If OSPF still cannot discover the remote routes after the above procedure is performed, check the following configurations:

- If two or more areas are configured on a router, at least one area should be configured to be connected to the backbone area.

As shown in Figure 75, Router A and Router D are configured to belong to only one area, whereas Router B (Area 0 and Area 1) and Router C (Area 1 and Area 2) are configured to belong to two areas. Router B also belongs to area 0, which meets the requirement. However, none of the areas of Router C is Area 0. Therefore, a virtual link should be set up between Router C and Router B. Ensure that Area 2 and Area 0 (backbone area) are interconnected.

Figure 75 OSPF area



- A virtual link cannot pass through a stub area. The backbone area (Area 0) cannot be configured as a stub area. So, if a virtual link has been set up between RTB and RTC, neither Area 1 nor Area 0 can be configured as a stub area. In Figure 75, only Area 2 can be configured as a stub area.
- A router in a stub area cannot receive external routes.
- The backbone area must guarantee the connectivity between various nodes.

35 IS-IS CONFIGURATION

IS-IS Overview

The intermediate system-to-intermediate system (IS-IS) is a dynamic routing protocol standardized by the International Organization for Standardization (ISO) to operate on connectionless network protocol (CLNP).

The IS-IS routing protocol has been adopted in RFC 1195 by the International Engineer Task Force (IETF) to be applied in both TCP/IP and OSI reference models, and this form is called Integrated IS-IS or Dual IS-IS.

The IS-IS routing protocol, based on the link state algorithm, is an interior gateway protocol (IGP) used within an Autonomous System. It is similar to open shortest path first (OSPF) using shortest path first (SPF) algorithm to calculate best paths in the network.

Basic Concept

IS-IS terminology

- Intermediate system (IS). An IS, similar to a router in TCP/IP, is the basic unit in IS-IS protocol to generate and propagate routing information. In the following text, an IS equals to a router.
- End system (ES). An ES refers to a host system in TCP/IP. ISO uses ES-IS protocol to specify the communication between an ES and an IS, therefore an ES does not participate in the IS-IS process and can be ignored in the IS-IS protocol.
- Routing domain (RD). A group of ISs exchange routing information with the same routing protocol in a routing domain.
- Area. An area is a division unit in a routing domain. The IS-IS protocol allows a routing domain to be divided into multiple areas.
- Link state database (LSDB). All link states in the network consist of the LSDB. There is at least one LSDB in each IS. The IS uses SPF algorithm and LSDB to generate its own routes.
- Link state protocol data unit or link state packet (LSP). In the IS-IS routing protocol, each IS can generate a LSP which contains all the link state information of the IS. Each IS collects all the LSPs in the local area to generate its own LSDB.
- Network protocol data unit (NPDU). An NPDU is a network layer protocol packet in ISO, which is equivalent to an IP packet in TCP/IP.
- Designated IS. On a broadcast network, the designated router is also known as the designated IS or a pseudonode.
- Network service access point (NSAP). The NSAP is the ISO network layer address. It identifies an abstract network service access point and describes the network address in the ISO reference model.

IS-IS network types

IS-IS supports two network types:

- Broadcast networks, such as Ethernet and Token-Ring
- Point-to-point networks, such as PPP and HDLC

For non-broadcast multi-access (NBMA) network, such as ATM, you need to configure point-to-point or broadcast network on its sub-interfaces. IS-IS does not run on point to multipoint (P2MP) links.

IS-IS Domain (Area)

Two-level hierarchy

The IS-IS uses two-level hierarchy in the routing domain to support large scale routing networks. A large routing domain is divided into multiple Areas. The Level-1 router is in charge of forwarding routes within an area, and the Level-2 router is in charge of forwarding routes between areas.

Level-1 and Level-2

1 Level-1 router

The Level-1 router only forms the neighbor relationship with Level-1 and Level-1-2 routers in the same area. The LSDB maintained by the Level-1 router contains the local area routing information. It directs the packets out of the area to the nearest Level-1-2 router.

2 Level-2 router

The Level-2 router forms the neighbor relationship with the Level-2 and Level-1-2 routers in the same or in different areas. It maintains a Level-2 LSDB which contains routing information for routing between areas. All Level-2 routers must be contiguous to form the backbone in a routing domain. Only Level-2 routers can directly communicate with routers outside the routing domain.

3 Level-1-2 router

A router functions as a Level-1 and a Level-2 router is called a Level-1-2 router. It can form the Level-1 neighbor relationships with the Level-1 and Level-1-2 routers in the same area, or form Level-2 neighbor relationships with the Level-2 and Level-1-2 routers in the same area or in different areas. A Level-1 router can be connected to other areas only via a Level-1-2 router. The Level-1-2 router maintains two LSDBs, where the Level-1 LSDB is for routing within the area, and the Level-2 LSDB is for routing between areas.



Level-1 routers in different areas cannot form neighbor relationships.

Level-2 routers in different areas can form neighbor relationships.

Figure 76 shows a network topology running the IS-IS protocol. Area 1 is a set of the Level-2 routers, called backbone network. The other four areas are non-backbone networks connected to the backbone through Level-1-2 routers.

Figure 76 IS-IS topology I

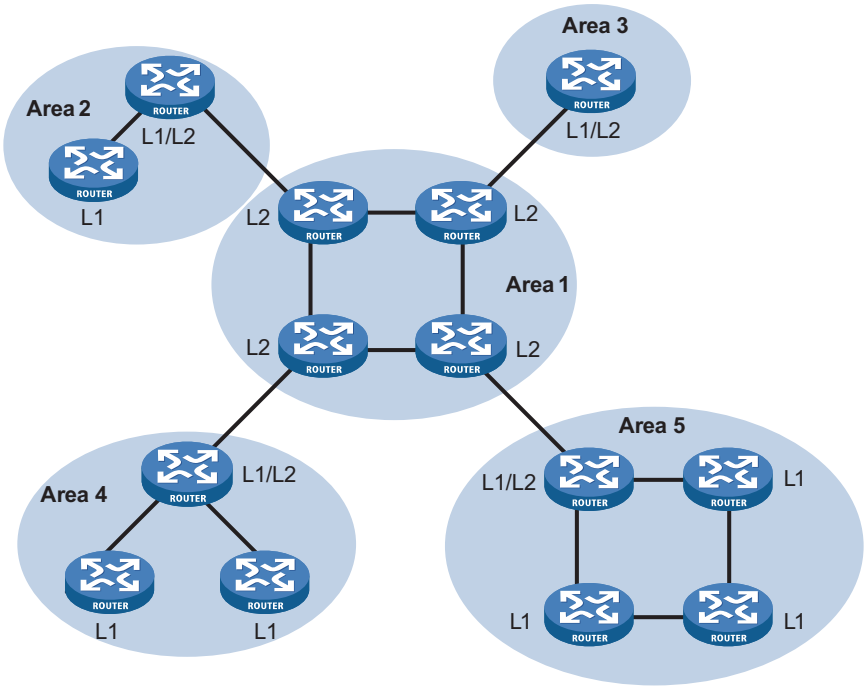
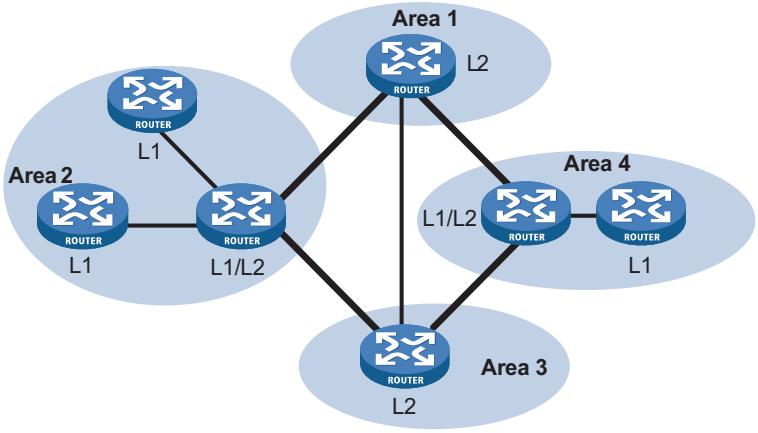


Figure 77 shows another IS-IS network topology. The Level-1-2 routers connect the Level-1 and Level-2 routers, and form the IS-IS backbone together with the Level-2 routers. There is no area defined as the backbone in this topology. The backbone is composed of all contiguous Level-2 and Level-1-2 routers which can reside in different areas.

Figure 77 IS-IS topology II



The IS-IS backbone does not need to be a specific area.

Both the IS-IS Level-1 and Level-2 routers use the SPF algorithm to generate the shortest path tree (SPT).

IS-IS Address Structure

Address structure

1 NSAP

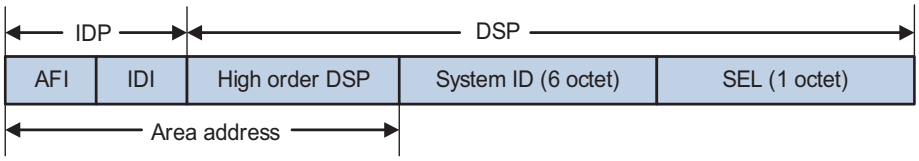
As shown in Figure 78, an NSAP address consists of the initial domain part (IDP) and the domain specific part (DSP). The IDP is equal to the network id field in the IP address, and the DSP is equal to the subnet and host id field.

The IDP, defined by ISO, includes the authority and format identifier (AFI) and the initial domain identifier (IDI).

The DSP includes the high order DSP (HODSP), System ID and SEL, where the HODSP identifies the area, the System ID identifies the host, and the SEL indicates the type of service.

The lengths of IDP and DSP are variable. The length of an NSAP address varies from 8 bytes to 20 bytes.

Figure 78 NSAP address structure



2 Area address

The area address is composed of the IDP and the HODSP of the DSP, which identify the area and the routing domain.

In normal condition, a router only needs one area address, and all nodes must share the same area addresses in the same domain. But a router can have three area addresses at most to support smooth area merging, partitioning and switching.

3 System ID

The system ID identifies the host or router uniquely. The Switch 7750 implement a fixed length of 48 bits (6 bytes).

The system ID is used in cooperate with the Router ID in practical. For example, a router uses the IP address 168.10.1.1 of the Loopback 0 as the Router ID, you can get the system ID used in IS-IS though the following method:

- Extend each field of the IP address to 3 digits with putting 0s from the left, like 168.010.001.001;
- Divide the extended IP address into 3 sections with 4 digits in each section, so the System ID is 1680.1000.1001.

There are other methods to define a system ID. Just make sure it can uniquely identify the host or router.

4 SEL

The NSAP Selector (SEL), sometimes present in N-SEL, is used as the protocol identifier in IP. Different transmission protocols use different SELs. All SELs in IP are 00.

Because the area is explicitly defined in the address structure, the Level-1 router can easily recognize the packets sent out of the area. Those packets are forwarded to the Level-2 router.

The Level-1 router makes routing decisions based on the system ID. If the destination is not in the area, the packet is forwarded to the nearest Level-1-2 router.

NET

The network entity title (NET) is an NSAP with SEL of 0. It indicates the network layer information of the IS itself. SEL=0 means it provides no transport layer information.

In normal condition, a router only needs one NET. But a router can have three NETs at most for smooth area merging and partitioning. When you configure multiple NETs, make sure their system IDs are same.

For example, there is a NET named 47.0001.aaaa.bbbb.cccc.00, where:

Area=47.0001, System ID=aaaa.bbbb.cccc,SEL=00.

Here is another example. A NET exists that is named 01.1111.2222.4444.00, where:

Area=01, System ID=1111.2222.4444, SEL=00.

IS-IS PDU Format

Hello

The Hello packet is used by routers to establish and maintain the neighbor relationship. It is also called IS-to-IS Hello PDUs (IIH). For broadcast network, the Level-1 router uses the Level-1 LAN IIH; and the Level-2 router uses the Level-2 LAN IIH. The P2P IIH is used on point-to-point network. Point-to-Point IIH is used on a non-broadcast network.

LSP packet format

The link state PDUs (LSP) carries link state information. There are two types: Level-1 LSP and Level-2 LSP. The Level-2 LSP is sent by the Level-2 router, and the Level-1 LSP is sent by the Level-1 router. The level-1-2 router can sent both types of the LSPs.

SNP format

The sequence number PDUs (SNP) confirms the latest LSPs received by neighbors. It is similar to the Acknowledge packet, but more efficient.

The SNP contains the complete SNP (CSNP) and the partial SNP (PSNP), which are further divided into Level-1 CSNP, Level-2 CSNP, Level-1 PSNP and Leval-2 PSNP.

Introduction to IS-IS Configuration

Table 251 IS-IS configuration tasks

Configuration Task		Description	Related section
Integrated IS-IS configuration	Enable IS-IS.	Required	"Enabling IS-IS" on page 334
	Configure a NET	Required	"Configuring a NET" on page 334
	Enable IS-IS on the specified interface	Required	"Enabling IS-IS on the Specified Interface" on page 334
	Configure DIS priority	Optional	"Configuring DIS Priority" on page 334
	Configure router type	Optional	"Configuring Router Type" on page 335
	Configure the line type of an interface	Optional	"Configuring the Line Type of an Interface" on page 335
	Configure route redistribution	Optional	"Configuring IS-IS Route Redistribution" on page 335
	Configure route filtering	Optional	"Configuring Route Filtering" on page 336
	Configure route leaking	Optional	"Configuring Route Leaking" on page 337
	Configure route summarization	Optional	"Configuring Route Summarization" on page 337
	Configure default route generation	Optional	"Configuring Default Route Generation" on page 337
	Configure protocol priority	Optional	"Configuring Protocol Priority" on page 337
	Configure a cost style	Optional	"Configuring a Cost Style" on page 338
	Configure interface cost	Optional	"Configuring Interface Cost" on page 338
	Configure IS-IS timer	Optional	"Configuring IS-IS Timer" on page 338
	Configure authentication	Optional	"Configuring Authentication" on page 340
	Add an interface to a mesh group	Optional	"Adding an Interface to a Mesh Group" on page 341

Table 251 IS-IS configuration tasks

Configuration Task	Description	Related section
Configure overload tag	Optional	"Configuring Overload Tag" on page 342
Configure to discard LSPs with incorrect checksum	Optional	"Configuring to Discard LSPs with Incorrect Checksum" on page 342
Configure to log peer changes	Optional	"Configuring to Log Peer Changes" on page 342
Assign an LSP refresh time	Optional	"Assigning an LSP Refresh Time" on page 342
Configure LSP maximum aging time	Optional	"Assigning an LSP Maximum Aging Time" on page 343
Configure SPF parameters	Optional	"Configuring SPF Parameters" on page 343
Enable/disable packet transmission through an interface	Optional	"Enabling/Disabling Packet Transmission Through an Interface" on page 344
Clear all IS-IS configuration data	Optional	"Resetting all IS-IS Configuration Data" on page 344
Reset configuration data of an IS-IS peer	Optional	"Resetting Configuration Data of an IS-IS Peer" on page 345

IS-IS Basic Configuration

All configuration tasks, except enabling IS-IS, are optional.

This section covers the following topics:

1 IS-IS basic configuration
- Enabling IS-IS
- Configuring a NET
- Enabling IS-IS on the specified interface
- Configuring DIS priority
- Configuring router type
- Configuring line type of an interface

2 IS-IS route configuration
- Configuring route redistribution
- Configuring route filtering
- Configuring route leaking
- Configuring route summarization
- Configuring default route generation

3 IS-IS-related configuration:
- Configuring IS-IS priority
- Configuring IS-IS timers

- Configuring routing cost type
- Configuring link state routing cost
- Configuring LSP parameters
- Configuring SPF parameters

4 Networking configuration

- Configuring authentication
- Configuring overload tag
- Configuring adjacency state output
- Configuring mesh group for an interface
- Disabling the sending of IS-IS packets

5 Some operation commands

- Clearing IS-IS data structure
- Clearing IS-IS specific neighbor

Enabling IS-IS

IS-IS can be enabled only after you create an IS-IS routing process and enable this routing process on the interfaces that may be associated with other routers.

Table 252 Enabling IS-IS

Operation	Command	Description
Enter system view	**system-view**	-
Configure ISIS	**isis** [*tag*]	Required By default, no IS-IS routing process is enabled.

Configuring a NET

A NET defines the current IS-IS area address and router system ID.

Table 253 Configure a NET

Operation	Command	Description
Enter system view	**system-view**	-
Enter IS-IS view	**isis** [*tag*]	-
Enable network entity	**network-entity** *net*	Required

Enabling IS-IS on the Specified Interface

Table 254 Enable IS-IS on the specified interface

Operation	Command	Description
Enter system view	**system-view**	-
Enter interface view	**interface** *interface-type interface-number*	Required
Enable IS-IS.	**isis enable** [**clns** | **ip**] [*tag*]	Required

Configuring DIS Priority

In a broadcast network, IS-IS needs to select a router as DIS.

When a DIS needs to be selected from the IS-IS neighbors on the broadcast network, the Level-1 DIS and Level-2 DIS should be selected respectively. The

higher priority a DIS has, the more likely it is to be chosen. If two or more routers with the highest priorities exist on the broadcast network, the router that has the greatest MAC address will be chosen. For adjacent routers that have the same priority of 0, the router that has the greatest MAC address will still be chosen.

Level-1 DIS and Level-2 DIS are selected respectively. You can set different priorities for DISs at different levels to be selected.

Table 255 Configure DIS priority

Operation	Command	Description
Enter system view	**system-view**	-
Enter interface view	**interface** *interface-type interface-number*	-
Assign a DIS priority	**isis dis-priority** *value* [**level-1** | **level-2**]	Optional The default DIS priority is 64.

Configuring Router Type

Table 256 Configure router type

Operation	Command	Description
Enter system view	**system-view**	-
Enter IS-IS view	**isis** [*tag*]	Required
Configure router type	**is-level** { **level-1** | **level-1-2** | **level-2** }	Optional By default, the router type is **level-1-2**.



Changing interface line type makes sense only when the interface is on a Level-1-2 router. Otherwise, the router type determines the adjacency hierarchy that can be established.

Configuring the Line Type of an Interface

Table 257 Configure the interface line type

Operation	Command	Description
Enter system view	**system-view**	-
Enter interface view	**interface** *interface-type interface-number*	Required
Configure the line type of an interface	**isis circuit-level** [**level-1** | **level-1-2** | **level-2**]	Optional The default line type is **level-1-2**.



Changing interface line type makes sense only when the interface is on a Level-1-2 router. Otherwise, the router type determines the adjacency hierarchy that can be established.

Configuring IS-IS Route Redistribution

IS-IS processes the routes discovered by other routing protocols as routes outside a routing domain. You can specify the default cost for IS-IS to redistribute routes from another routing protocol.

You can configure IS-IS to redistribute routes to Level-1, Level-2, and Level-1-2.

Table 258 Configure route redistribution

Operation	Command	Description
Enter system view	**system-view**	-
Enter IS-IS view	**isis** [*tag*]	Required
Enable route redistribution from another routing protocol	**import-route** *protocol* [**allow-ibgp**] [**cost** *value* | **type** { **external** | **internal** } | [**level-1** | **level-1-2** | **level-2**] | **route-policy** *route-policy-name*]*	Optional By default, no route redistribution is configured.

- *For more information about route redistribution, refer to "IP Routing Policy Configuration" on page 378.*
- *The **allow-ibgp** keyword is used to redistribute iBGP routes. Because the AS-PATH attribute of redistributed iBGP routes is discarded, routing loops may occur. Therefore, use this keyword with caution.*

Configuring Route Filtering

IS-IS can filter received routes and advertised routes based on ACL numbers.

Configuring received route filtering

Table 259 Configure received route filtering

Operation	Command	Description
Enter system view	**system-view**	-
Enter IS-IS view	**isis** [*tag*]	Required
Set the policy for filtering received routes	**filter-policy** *acl-number* **import**	Required By default, IS-IS does not filter received routes.

Configuring IS-IS to filter the routes advertised by other routing protocols

Table 260 Configure IS-IS to filter the routes advertised by other routing protocols

Operation	Command	Description
Enter system view	**system-view**	-
Enter IS-IS view	**isis** [*tag*]	Required
Set the policy for filtering the routes advertised by other protocols	**filter-policy** *acl-number* **export** [*protocol*]	Optional By default, IS-IS does not receive the routes advertised by other routing protocols.

- *The **filter-policy import** command filters only the IS-IS routes received from neighbors. The routes that cannot pass the filtering will not be added to the routing table.*
- *The **filter-policy export** command only applies to the routes imported with the **import-route** command. The **filter-policy export** command will not work if you do not configure the **import-route** command to import non-IS-IS routes.*
- *If you do not specify which type of routes are to be filtered with the **filter-policy export** command, all the routes imported with the **import-route** command will be filtered.*

Configuring Route Leaking

Through route leaking, a Level-2 router can send the Level-1 area routing information and Level-2 area routing information that it knows to a Level-1 router.

Table 261 Configure route leaking

Operation	Command	Description
Enter system view	**system-view**	-
Enter IS-IS view	**isis** [*tag*]	Required
Enable route leaking	**import-route isis level-2 into level-1** [**acl** *acl-number*]	Optional By default, a Level-2 router sends no routing information to a Level-1 area.

Configuring Route Summarization

You can configure the routes having the same IP prefix as one summarized route.

Table 262 Configure route summarization

Operation	Command	Description
Enter system view	**system-view**	-
Enter IS-IS view	**isis** [*tag*]	Required
Configure route summarization	**summary** *ip-address ip-mask* [**level-1** | **level-1-2** | **level-2**]	Optional By default, the system performs no route summarization.

Configuring Default Route Generation

In an IS-IS routing domain, a Level-1 router maintains the LSDB for the local area only and generates the routes within the local area only. A Level-2 router maintains the LSDB for the backbone within the IS-IS routing domain and generates the routes for the backbone only. To transfer packets to another area, a Level-1 router in an area needs to first transfer the packets to the nearest Level-1-2 router within the local area. This requires the default route at Level-1.

Table 263 Configure default route generation

Operation	Command	Description
Enter system view	**system-view**	-
Enter IS-IS view	**isis** [*tag*]	Required
Configure default route generation	**default-route-advertise** [**route-policy** *route-policy-name*]	Optional The default route is advertised to only the routers at the same level.

Configuring Protocol Priority

For a router running multiple routing protocols, routing information needs to be shared and selected by the routing protocols. The system assigns a priority for each routing protocol. When multiple routing protocols discover a route to the same destination, the protocol with the highest priority will dominate.

Table 264 Configure protocol priority

Operation	Command	Description
Enter system view	**system-view**	-
Enter IS-IS view	**isis** [*tag*]	Required

Table 264 Configure protocol priority

Operation	Command	Description
Configure protocol priority	**preference** [*value* | **clns** | **ip**] *value*	Optional The default priority of IS-IS routes is 15.

Configuring a Cost Style

In IS-IS routing protocol, routing cost of a link can be expressed in one of the following two modes:

- Narrow: In this mode, routing cost ranges from 1 to 63.
- Wide: In this mode, routing cost ranges from 1 to 2^{24}-1, namely, 1 to 16777215.

You can specify to support either mode or both.

Table 265 Configure IS-IS route cost style

Operation	Command	Description
Enter system view	**system-view**	-
Enter IS-IS view	**isis** [*tag*]	Required
Configure a cost style	**cost-style** { **narrow** | **wide** | **wide-compatible** | { **compatible** | **narrow-compatible** } [**relax-spf-limit**] }	Optional By default, IS-IS receives/sends only the packets with routing cost expressed in the Narrow mode.

Configuring Interface Cost

Table 266 Configure interface cost

Operation	Command	Description
Enter system view	**system-view**	-
Enter interface view	**interface** *interface-type interface-number*	Required
Configure interface cost	**isis cost** *value* [**level-1** | **level-2**]	Optional The default IS-IS interface cost is 10.

Configuring IS-IS Timer

Configuring the Hello interval

In IS-IS, Hello packets are sent periodically through interfaces and routers maintain neighbor relationship by sending and receiving Hello packets. You can configure the Hello interval.

Table 267 Configure the Hello interval

Operation	Command	Description
Enter system view	**system-view**	-
Enter interface view	**interface** *interface-type interface-number*	Required

Table 267 Configure the Hello interval

Operation	Command	Description
Define the Hello packet sending interval, in seconds	**isis timer hello** *seconds* [**level-1** | **level-2**]	Optional The default Hello packets sending interval is 10 seconds.

Configuring the CSNP packets sending interval

CSNP packets are the packets sent with the synchronous LSDB by the DIS on a broadcast network. CSNP packets are broadcast periodically on a broadcast network. You can configure the interval of sending CSNP packets.

Table 268 Configure the CSNP packets sending interval

Operation	Command	Description
Enter system view	**system-view**	-
Enter interface view	**interface** *interface-type interface-number*	Required
Configure the CSNP packets sending interval, in seconds	**isis timer csnp** *seconds* [**level-1** | **level-2**]	Optional The default CSNP packets sending interval is 10 seconds.

Configuring the LSP sending interval

LSPs are used to advertise link state records within an area.

Table 269 Configure the LSP sending interval

Operation	Command	Description
Enter system view	**system-view**	-
Enter interface view	**interface** *interface-type interface-number*	Required
Configure the LSP sending interval, in milliseconds	**isis timer lsp** *time*	Optional The default LSP sending interval is 33 milliseconds.

Configuring the LSP retransmitting interval on an interface

On a point-to-point link, if there is no response for the sent LSP, the LSP is considered lost or discarded and the sending router retransmits the LSP.

Table 270 Configure LSP retransmitting interval

Operation	Command	Description
Enter system view	**system-view**	-
Enter interface view	**interface** *interface-type interface-number*	Required
Configure the LSP retransmitting interval on a point-to-point link<	**isis timer retransmit** *seconds*	Optional By default, LSPs are retransmitted on a point-to-point link every five seconds.

Configuring the number of Hello packets expected from the remote router before it is considered dead

In IS-IS, Hello packets are sent and received to maintain router neighbor relationships. If a router does not receive any Hello packet from a neighboring router in a certain period of time (Holddown time in IS-IS), the neighbor is considered dead.

In IS-IS, you can adjust the Holddown time by configuring the number of Hello packets expected from a neighbor router before it is considered dead.

Table 271 Configure the number of Hello packets expected from the remote router before it is considered dead

Operation	Command	Description
Enter system view	**system-view**	-
Enter interface view	**interface** *interface-type interface-number*	Required
Configure the number of Hello packets expected from the remote router before it is considered dead	**isis timer holding-multiplier** *value* [**level-1** | **level-2**]	Optional By default, three Hello packets are expected from the remote router before it is considered dead.

*If you do not provide the **level-1** keyword or the **level-2** keyword, this command applies to Level-1 and Level-2.*

Configuring Authentication

Configuring authentication on an interface

The authentication configured on the interface applies to the Hello packet in order to authenticate neighbors. All interfaces must share the same authentication password in the same level within a network.

Table 272 Configure authentication

Operation	Command	Description
Enter system view	**system-view**	-
Enter interface view	**interface** *interface-type interface-number*	Required
Configure the IS-IS authentication mode and password	**isis authentication-mode** { **simple** | **md5** } *password* [{ **level-1** | **level-2** } [**ip** | **osi**]]	Optional By default, no authentication is configured.

Configuring authentication for an IS-IS area or routing domain

You can configure an authentication password for an IS-IS area or routing domain.

If area authentication is required, the area authentication password is encapsulated in the LSP, CSNP, and PSNP packets at Level-1 as predefined. If area authentication is also enabled on other routers in the same area, area authentication works normally only if the authentication mode and password of these routers are the same as those of the neighboring routers.

Likewise, if domain authentication is required, the domain authentication password is also encapsulated in the LSP, CSNP, and PSNP packets at Level-2 as

predefined. If domain authentication is also required on other routers at the backbone layer (Level-2), the authentication works normally only if the authentication mode and password of these routers are the same as those of the neighboring routers.

Table 273 Configure authentication

Operation	Command	Description
Enter system view	**system-view**	-
Enter IS-IS view	**isis** [*tag*]	Required
Define the area authentication mode	**area-authentication-mode** { **simple** | **md5** } *password* [**ip** | **osi**]	Optional
Define the domain authentication mode	**domain-authentication-mode** { **simple** | **md5** } *password* [**ip** | **osi**]	Optional By default, no password is defined and no authentication is enabled.

Configuring IS-IS to use an MD5 algorithm compatible with the switches of other manufacturers

To enable IS-IS MD5 authentication between the switch and the switches of other manufacturers, you must use the following commands to configure IS-IS to use an MD5 algorithm compatible with the switches of other manufacturers.

Table 274 Configure IS-IS to use an MD5 algorithm compatible with the switches of other manufacturers

Operation	Command	Description
Enter system view	**system-view**	-
Enter IS-IS view	**isis** [*tag*]	Required
Configure IS-IS to use an MD5 algorithm compatible with the switches of other manufacturers	**md5-compatible**	Optional
Configure IS-IS to use the default MD5 algorithm	**undo md5-compatible**	Optional By default, the private MD5 algorithm is used.

Adding an Interface to a Mesh Group

On an NBMA network, a router floods a new LSP received from an interface to other interfaces of the router. This can cause repeated LSP flooding on a high-connectivity network with multiple point-to-point links, which is a waste of the bandwidth.

To avoid this problem, you can add interfaces into a mesh group. The interfaces in the group will flood the new LSPs to only the interfaces outside the mesh group.

Table 275 Add an interface to a mesh group

Operation	Command	Description
Enter system view	**system-view**	-
Enter interface view	**interface** *interface-type interface-number*	Required

Table 275 Add an interface to a mesh group

Operation	Command	Description
Add an interface to a mesh group	**isis mesh-group** { *mesh-group-number* | **mesh-blocked** }	Optional By default, LSPs are flooded on interfaces normally.

Configuring Overload Tag

A failure of a router in an IS-IS domain will cause errors in the routing of the whole domain. To avoid this, you can configure the overload for the routers.

When the overload tag is set, other routers will not ask the router to forward packets.

Table 276 Configure overload tag

Operation	Command	Description
Enter system view	**system-view**	-
Enter IS-IS view	**isis** [*tag*]	Required
Configure overload tag	**set-overload**	Optional No overload tag is set by default.

Configuring to Discard LSPs with Incorrect Checksum

Checksum is performed on the LSPs received locally by IS-IS and compared with that carried in the LSPs By default, the LSP will not be discarded even if its checksum is inconsistent with that calculated. You can use the **ignore-lsp-checksum-error** command to configure IS-IS to discard an LSP with incorrect checksum.

Table 277 Configure to discard LSPs with incorrect checksum

Operation	Command	Description
Enter system view	**system-view**	-
Enter IS-IS view	**isis** [*tag*]	Required
Configure to discard LSPs with incorrect checksum	**ignore-lsp-checksum-error**	Optional By default, LSP checksum error is ignored.

Configuring to Log Peer Changes

With peer state logging enabled, IS-IS peer state changes are output to the console terminal.

Table 278 Enable peer change logging

Operation	Command	Description
Enter system view	**system-view**	-
Enter IS-IS view	**isis** [*tag*]	Required
Enable peer change logging	**log-peer-change**	Optional By default, peer change logging is disabled.

Assigning an LSP Refresh Time

All LSPs are sent periodically to synchronize the LSPs in an area.

Table 279 Assign an LSP refresh time

Operation	Command	Description
Enter system view	**system-view**	-
Enter IS-IS view	**isis** [*tag*]	Required
Assign an LSP refresh time	**timer lsp-refresh** *seconds*	Optional By default, LSPs are refreshed every 900 seconds, namely, 15 minutes.

Assigning an LSP Maximum Aging Time

An LSP is given a maximum aging value when it is generated by the router. When the LSP is sent to other routers, its maximum aging value goes down gradually. If the router does not get the update for the LSP before the maximum aging value reaches 0, the LSP will be deleted from the LSDB.

Table 280 Assign an LSP maximum aging time

Operation	Command	Description
Enter system view	**system-view**	-
Enter IS-IS view	**isis** [*tag*]	Required
Assign an LSP maximum aging time	**timer lsp-max-age** *seconds*	Optional By default, the LSP maximum aging time is 1,200 seconds, namely, 20 minutes.

Configuring SPF Parameters

Configuring the SPF interval

In IS-IS, a router needs to recalculate the shortest path when the LSDB changes. Recalculating the shortest path upon change consumes enormous resources as well as affects the operation efficiency of the router. With an SPF calculation interval configured, when the LSDB changes, the SPF algorithm is not executed until the SPF timer expires.

Table 281 Configure the SPF interval

Operation	Command	Description
Enter system view	**system-view**	-
Enter IS-IS view	**isis** [*tag*]	Required
Configure the SPF interval	**timer spf** *seconds* [**level-1** | **level-2**]	Optional The default SPF interval is 10 seconds.

*If you do not provide the **level-1** or **level-2** keyword, this command applies to Level-1 and Level-2 by default.*

Configuring SPF calculation durations

SPF calculation in IS-IS may occupy system resources for a long time if the routing table contains a great number of entries (over 30,000). To avoid this, you can configure SPF calculation durations.

Table 282 Configure SPF calculation durations

Operation	Command	Description
Enter system view	**system-view**	-

Table 282 Configure SPF calculation durations

Operation	Command	Description
Enter IS-IS view	**isis** [*tag*]	Required
Configure SPF calculation duration	**spf-slice-size** *seconds*	Optional By default, SPF calculation is not sliced.

Configuring SPF to release CPU resources automatically

In IS-IS, SPF calculation may occupy system resources for a long time and slow down console response. To avoid this, you can configure SPF to automatically release CPU resources each time a specified number of routes are processed and continue to calculate the remaining routes after one second.

Table 283 Configure SPF to release CPU resources automatically

Operation	Command	Description
Enter system view	**system-view**	-
Enter IS-IS view	**isis** [*tag*]	Required
Configure the interval at which SPF releases CPU resources	**spf-delay-interval** *number*	Optional By default, in IS-IS, SPF releases CPU resources each time it has finished processing 5,000 routes.

Enabling/Disabling Packet Transmission Through an Interface

To prevent IS-IS routing information from being accessed by a router on another network, use the **silent-interface** command to configure the VLAN interface containing the network segment to receive, but not to send, IS-IS packets.

Table 284 Enable/disable packet transmission through an interface

Operation	Command	Description
Enter system view	**system-view**	-
Enter IS-IS view	**isis** [*tag*]	Required
Disable an interface from sending IS-IS packets	**silent-interface** *interface-type interface-number*	Optional By default, an interface is enabled to receive and send IS-IS packets.

Resetting all IS-IS Configuration Data

Perform the following configuration in user view to refresh LSPs immediately.

Table 285 Reset all IS-IS configuration data

Operation	Command	Description
Enter system view	**system-view**	-
Reset all IS-IS configuration data	**reset isis all**	Optional By default, IS-IS configuration data is not cleared.

Resetting Configuration Data of an IS-IS Peer

Table 286 Reset configuration data of the IS-IS peer

Operation	Command	Description
Enter system view	**system-view**	-
Reset configuration data of an IS-IS peer	**reset isis peer** *system-id*	Optional By default, configuration data of an IS-IS peer is not reset.

Displaying Integrated IS-IS Configuration

After the above-mentioned configuration, you can use the **display** command in any view to display the IS-IS running state.

By performing the following operations, you can display IS-IS link state database, packet transmission, and SPF calculation, so as to verify IS-IS route maintenance.

Table 287 Display and maintain integrated IS-IS configuration

Operation	Command	Description
Display brief information of IS-IS	**display isis brief**	You can execute the **display** command in any view.
Display IS-IS link state database	**display isis lsdb** [[**l1** | **l2** | **level-1** | **level-2**] | [[*lsp-id* | **local**] | **verbose**]*]*	
Display IS-IS SPF logs	**display isis spf-log** { **ip | clns** }	
Display IS-IS routes	**display isis route**	
Display IS-IS peer information	**display isis peer** [**verbose**]	
Display mesh group information	**display isis mesh-group**	
Display IS-IS interface information	**display isis interface** [**verbose**]	

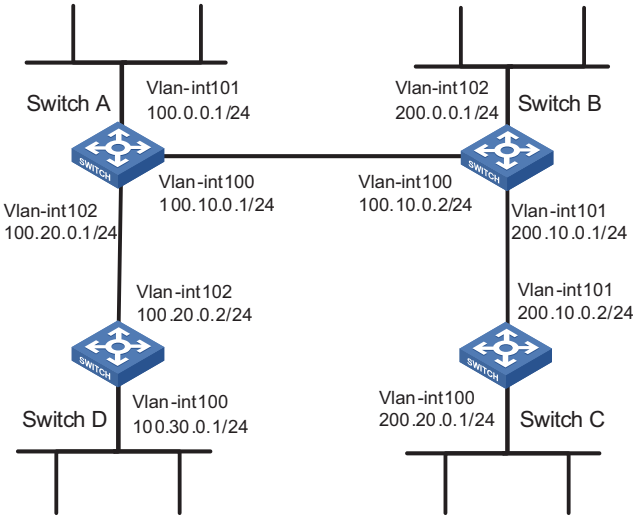
Integrated IS-IS Configuration Example

Network requirements

As shown in Figure 79, four Switch 7750 Ethernet switches (Switch A, Switch B, Switch C, and Switch D) are interconnected through IS-IS routing protocol. In the network design, Switch A, Switch B, Switch C, and Switch D belong to the same area.

Network diagram

Figure 79 Network diagram for IS-IS basic configuration



Configuration procedure

Configure Switch A.

```
<SwitchA> system-view
[SwitchA] isis
[SwitchA-isis] network-entity 86.0001.0000.0000.0005.00
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ip address 100.10.0.1 255.255.255.0
[SwitchA-Vlan-interface100] isis enable
[SwitchA] interface vlan-interface 101
[SwitchA-Vlan-interface101] ip address 100.0.0.1 255.255.255.0
[SwitchA-Vlan-interface101] isis enable
[SwitchA] interface vlan-interface 102
[SwitchA-Vlan-interface102] ip address 100.20.0.1 255.255.255.0
[SwitchA-Vlan-interface102] isis enable
```

Configure Switch B.

```
[SwitchB] isis
[SwitchB-isis] network-entity 86.0001.0000.0000.0006.00
[SwitchB] interface vlan-interface 101
[SwitchB-Vlan-interface101] ip address 200.10.0.1 255.255.255.0
[SwitchB-Vlan-interface101] isis enable
[SwitchB] interface vlan-interface 102
[SwitchB-Vlan-interface102] ip address 200.0.0.1 255.255.255.0
[SwitchB-Vlan-interface102] isis enable
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ip address 100.10.0.2 255.255.255.0
[SwitchB-Vlan-interface100] isis enable
```

Configure Switch C.

```
[SwitchC] isis
[SwitchC-isis] network-entity 86.0001.0000.0000.0007.00
[SwitchC] interface vlan-interface 101
[SwitchC-Vlan-interface101] ip address 200.10.0.2 255.255.255.0
```

```
[SwitchC-Vlan-interface101] isis enable
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] ip address 200.20.0.1 255.255.255.0
[SwitchC-Vlan-interface100] isis enable
```

Configure Switch D.

```
[SwitchD] isis
[SwitchD-isis] network-entity 86.0001.0000.0000.0008.00
[SwitchD] interface vlan-interface 102
[SwitchD-Vlan-interface102] ip address 100.20.0.2 255.255.255.0
[SwitchD-Vlan-interface102] isis enable
[SwitchD] interface vlan-interface 100
[SwitchD-Vlan-interface100] ip address 100.30.0.1 255.255.255.0
[SwitchD-Vlan-interface100] isis enable
```

36 BGP CONFIGURATION

BGP Overview

Introduction to BGP

Border gateway protocol (BGP) is a dynamic routing protocol designed to be used between autonomous systems (AS). An AS is a group of routers that adopt the same routing policy and belong to the same technical management department.

Four versions of BGP exist: BGP-1 (described in RFC1105), BGP-2 (described in RFC1163), BGP-3 (described in RFC1267), and BGP-4 (described in RFC1771). As the actual internet exterior routing protocol standard, BGP-4 is widely employed between internet service providers (ISP).



Unless otherwise noted, BGP in the following sections refers to BGP-4.

BGP is featured by the following.

- Unlike interior gateway protocols (IGP) such as OSPF (open shortest path first), RIP (routing information field), and so on, BGP is an exterior gateway protocol (EGP). It does not focus on discovering and computing routes but controlling the route propagation and choosing the optimal route.
- BGP uses TCP as the transport layer protocol (with the port number being 179) to ensure reliability.
- BGP supports classless inter-domain routing (CIDR).
- With BGP employed, only the changed routes are propagated. This saves network bandwidth remarkably and makes it feasible to propagate large amount of route information across the Internet.
- The AS path information used in BGP eliminates routing loops thoroughly.
- In BGP, multiple routing policies are available for filtering and choosing routes in a flexible way.
- BGP is extendible to allow for new types of networks.

In BGP, the routers that send BGP messages are known as BGP speakers. A BGP speaker receives and generates new routing information and advertises the information to other BGP speakers. When a BGP speaker receives a route from other AS, if the route is better than the existing routes or the route is new to the BGP speaker, the BGP speaker advertises the route to all other BGP speakers in the AS it belongs to.

A BGP speaker is known as the peer of another BGP speaker if it exchanges messages with the latter. A group of correlated peers can form a peer group.

BGP can operate on a router in one of the following forms.

- IBGP (Internal BGP)
- EBGP (External BGP)

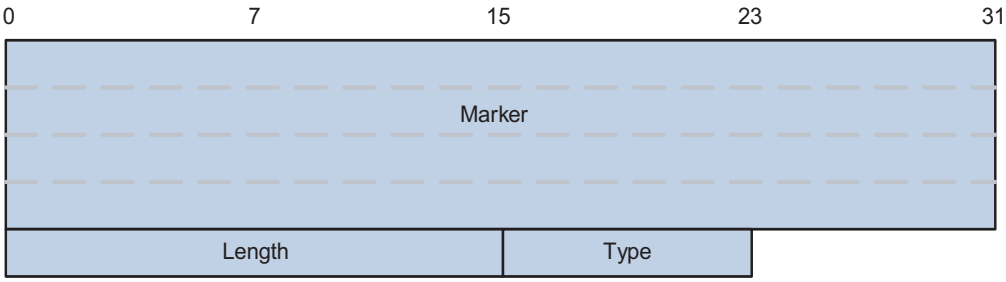
When BGP runs inside an AS, it is called interior BGP (IBGP); when BGP runs among different ASs, it is called exterior BGP (EBGP).

BGP Message Type

Format of a BGP packet header

BGP is message-driven. There are five types of BGP packets: Open, Update, Notification, Keepalive, and Route-refresh. They share the same packet header, the format of which is shown by Figure 80.

Figure 80 Packet header format of BGP messages



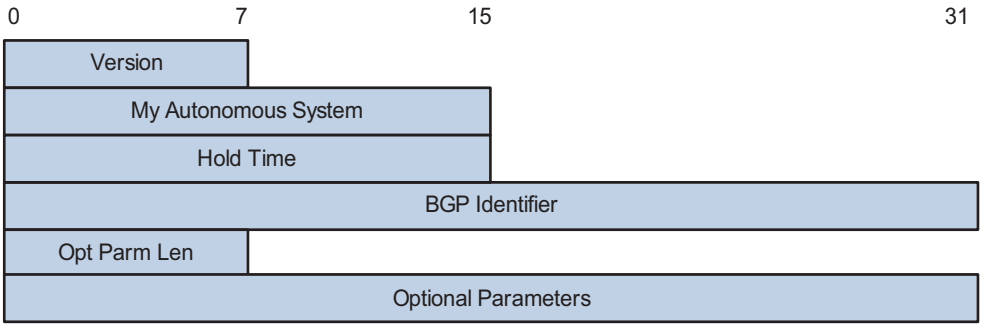
The fields in a BGP packet header are described as follows.

- Marker: 16 bytes in length. This filed is used for BGP authentication. When no authentication is performed, all the bits of this field are 1.
- Length: 2 bytes in length. This filed indicates the size (in bytes) of a BGP packet, with the packet header counted in.
- Type: 1 byte in length. This field indicates the type of a BGP packet. Its value ranges from 1 to 5, which represent Open, Update, Notification, Keepalive, and Route-refresh packets. Among these types of BGP packets, the first four are defined in RFC1771, and the rest one is defined in RFC2918.

Open

Open massage is used to establish connections between BGP speakers. It is sent when a TCP connection is just established. Figure 81 shows the format of an Open message.

Figure 81 BGP Open message format



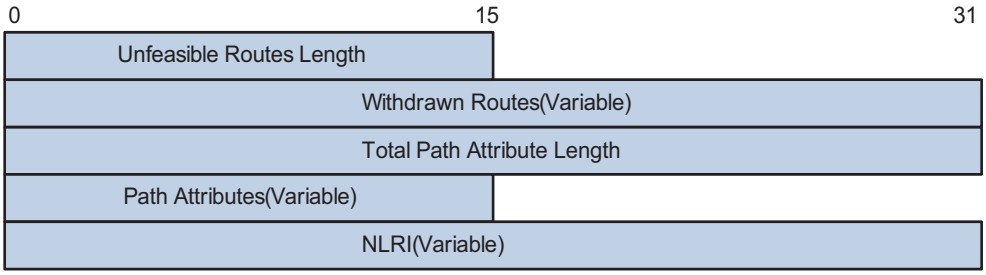
The fields are described as follows.

- Version: BGP version. As for BGP-4, the value is 4.
- My Autonomous System: Local AS number. By comparing this filed of both sides, a router can determine whether the connection between itself and the BGP peer is of EBGP or IBGP.
- Hold time: Hold time is to be determined when two BGP speakers negotiate for the connection between them. The Hold times of two BGP peers are the same. A BGP speaker considers the connection between itself and its BGP peer to be terminated if it receives no Keepalive or Update message from its BGP peer during the hold time.
- BGP Identifier: The IP address of a BGP router.
- Opt Parm Len: The length of the optional parameters. A value of 0 indicates no optional parameter is used.
- Optional Parameters: Optional parameters used for BGP authentication or multi-protocol extensions.

Update

Update message is used to exchange routing information among BGP peers. It can propagate a reachable route or withdraw multiple pieces of unreachable routes. Figure 82 shows the format of an Update message.

Figure 82 BGP Update message format



An Update message can advertise a group of reachable routes with the same path attribute. These routes are set in the NLRI field. The Path Attributes field carries the attributes of these routes, according to which BGP chooses routes. An Update message can also carry multiple unreachable routes. The withdrawn routes are set in the Withdrawn Routes field.

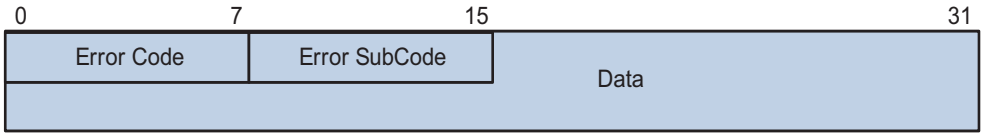
The fields of an Update message are described as follows.

- Unfeasible Routes Length: Length (in bytes) of the unreachable routes field. A value of 0 indicates that there is no Withdrawn Routes filed in the message.
- Withdrawn Routes: Unreachable route list.
- Total Path Attribute Length: Length (in bytes) of the Path Attributes field. A value of 0 indicates that there is no Path Attributes filed in the message.
- Path Attributes: Attributes list of all the paths related to NLRI. Each path attribute is a TLV (Type-Length-Value) triplet. In BGP, loop avoidance, routing, and protocol extensions are implemented through these attribute values.
- NLRI (Network Layer Reachability Information): Contains the information such reachable route suffix and the corresponding suffix length.

Notification

When BGP detects error state, it sends the Notification message to peers and then tear down the BGP connection. Figure 83 shows the format of an Notification message.

Figure 83 BGP Notification message format



The fields of a Notification message are described as follows.

- Error Code: Error code used to identify the error type.
- Error Subcode: Error subcode used to identify the detailed information about the error type.
- Data: Used to further determine the cause of errors. Its content is the error data which depends on the specific error code and error subcode. Its length is unfixed.

Keepalive

In BGP, Keepalive message keeps BGP connection alive and is exchanged periodically. A BGP Keepalive message only contains the packet header. No additional fields is carried.

Route-refresh

Route-refresh message is used to notify the peers that the route refresh function is available.

BGP Routing Mechanism

When BGP initially starts on a router, it sends the whole BGP routing table to its peers to exchange routing information. Afterwards, BGP sends only Update messages instead of the whole table. During the running, BGP also sends/receives Keepalive messages to determine whether the connections to its peers are normal.

A router running BGP is also called a BGP speaker because it can send BGP messages. A BGP speaker can receive routing information as well as generate and advertise routing information to other BGP speakers. When a BGP speaker receives a route from another AS and finds this is a new route (a route it does not know) or a route superior than any of its known routes, the BGP speaker advertises the route to all other BGP speakers in the AS.

Two BGP speakers capable of exchanging BGP messages with each other are peers of each other. Multiple BGP peers can form one peer group.

BGP route advertisement policies

In the implementation on the Switch 7750, BGP adopts the following policies to advertise routes:

- When there are multiple optional routes, a BGP speaker chooses only the optimal one;
- A BGP speaker advertises only the local routes to its peers;

- A BGP speaker advertises the routes obtained from EBGP to all its BGP peers (including both EBGP and IBGP peers);
- A BGP speaker does not advertise the routes obtained from IBGP to its IBGP peers;
- A BGP speaker advertises the routes obtained from IBGP to its EBGP peers (in Switch 7750, BGP and IGP does not synchronize with each other);
- Once a BGP speaker sets up a connection to a new peer, it advertises all its BGP routes to the new peer.

BGP route selection policies

In the implementation on Switch 7750, BGP adopts the following policies for route selection:

- Discard next-hop-unreachable routes;
- Prefer the routes with the highest local-preference;
- Prefer the routes initiated from the local router;
- Prefer the routes across the least ASs (that is, the routes with the shortest AS-Path);
- Prefer the routes with the lowest Origin type;
- Prefer the routes with the lowest MED value;
- Prefer the routes learned from EBGP;
- Prefer the routes advertised from the router with the lowest BGP ID.

BGP Peer and Peer Group

Definition

As described in "BGP Routing Mechanism" on page 352, two BGP speakers capable of exchanging BGP messages with each other are peers of each other. A BGP peer group is a set of BGP peers.

Relation between peer and peer group

In the Switch 7750, a BGP peer cannot exist independently; it must belong to a peer group. Therefore, when you configure a BGP peer, you must first create a BGP peer group, and then add a peer to the group.

BGP peer groups bring convenience for configuration. Once a peer is added to a peer group, the peer will inherit the same configuration of the peer group. This can simplify your configuration in many cases. In addition, adding peers to a peer group can improve route advertisement efficiency.

When the configuration of a peer group changes, the configuration of group members also changes in the same way. For some attributes, you can configure them on a particular member by specifying an IP address; and the attribute settings you made in this way on a member take precedence over the attribute settings on the peer group. Note that, the members and the group must have consistent route update policies, but they can have different entrance policies.

BGP Configuration Tasks

Table 288 BGP configuration tasks

Configuration task		Description	Related section
Basic BGP configuration		Required	"Basic BGP Configuration" on page 355
Configuring the way to advertise/receive routing information	Importing routes	Optional	"Importing Routes" on page 357
	Configuring route aggregation	Optional	"Configuring BGP Route Aggregation" on page 357
	Sending default routes	Optional	"Enabling Default Route Advertising" on page 358
	Configuring advertising policy for BGP routing information	Optional	"Configuring the BGP Route Advertising Policy" on page 358
	Configuring receiving policy for BGP routing information	Optional	"Configuring BGP Route Receiving Policy" on page 359
	Configuring BGP-IGP Route Synchronization	Optional	"Configuring BGP-IGP Route Synchronization" on page 360
	Configuring BGP route dampening	Optional	"Configuring BGP Route Dampening" on page 360
	Configuring BGP load balance	Optional	"Configuring BGP Load Balance" on page 361
Configuring BGP route attributes		Optional	"Configuring BGP Route Attributes" on page 361
Adjusting and optimizing a BGP network		Optional	"Adjusting and Optimizing a BGP Network" on page 363
Configure a large-scale BGP network	Configuring a BGP peer group	Required	"Configuring BGP Peer Group" on page 365
	Configuring a BGP community	Required	"Configuring BGP Community" on page 366
	Configuring BGP RR	Optional	"Configuring BGP RR" on page 367
	Configure BGP confederation	Optional	"Configuring BGP Confederation" on page 367

Basic BGP Configuration

Configuration Prerequisites

Before performing basic BGP configuration, you need to ensure:

- Network layer connectivity between adjacent nodes.

Before performing basic BGP configuration, make sure the following are available.

- Local AS number and router ID
- IPv4 address and AS number of the peers
- Source interface of update packets.

Configuring BGP Multicast Address Family

Table 289 Configure BGP multicast address family

Operation	Command	Description
Enter system view	**system-view**	-
Start BGP and enter BGP view	**bgp** *as-number*	Required By default, the system does not run BGP.
Enter multicast address family view	**ipv4-family multicast**	Required

Commands are configured in a similar way in multicast address family view and in BGP view. Unless otherwise specified, follow the configuration in BGP view. For details, see the corresponding command manual. All the following uses the configuration in BGP view for example.

Configuring Basic BGP Functions

Table 290 Configure basic BGP functions

Operation	Command	Description
Enter system view	**system-view**	-
Specify the router ID	**router id** *ip-address*	Optional
Enable BGP and enter BGP view	**bgp** *as-number*	Required By default, BGP is disabled.
Create a peer group	**group** *group-name* [**internal** | **external**]	Required
Add a peer to the peer group	**peer** *peer-address* **group** *group-name* [**as-number** *as-number*]	Required If it is an IBGP peer, you need not specify an AS number.
Set an AS number for the peer group	**peer** *group-name* **as-number** *as-number*	Required By default, a peer group has no AS number.
Assign a description string for a BGP peer/a BGP peer group	**peer** { *group-name* | *ip-address* } **description** *description-text*	Optional By default, a peer/a peer group is not assigned a description string.
Activate a specified BGP peer	**peer** { *group-name* | *ip-address* } **enable**	Required

Table 290 Configure basic BGP functions

Operation	Command	Description
Specify the source interface for route update packets	**peer** { *group-name* | *ip-address* } **connect-interface** *interface-type interface-number*	Optional By default, the source interface of the optimal route update packets is used.
Allow routers that belong to non-directly connected networks to establish EBGP connections.	**peer** *group-name* **ebgp-max-hop** [*hop-count*]	Optional By default, routers that belong to two non-directly connected networks cannot establish EBGP connections. You can configure the maximum hops of EBGP connection by specifying the *hop-count* argument.

CAUTION:

- *A router must be assigned a router ID in order to run BGP protocol. A router ID is a 32-bit unsigned integer. It uniquely identifies a router in an AS.*
- *A router ID can be configured manually. If no router ID is configured, the system will automatically select an IP address from the IP addresses of the interfaces as the router ID. A router ID is selected in the following way: if loopback interface addresses are configured, the system chooses the latest configured IP address as the router ID; if no loopback interface is configured, the first configured IP address among the IP addresses of other interfaces will be the router ID. For network reliability consideration, you are recommended to configure the IP address of a loopback interface as the router ID.*
- *Router IDs can be re-selected. A re-selected router ID takes effect only after the BGP process is restarted.*
- *Normally, EBGP peers are connected through directly connected physical links. If no such link exists, you need to use the* ***peer ebgp-max-hop*** *command to allow the peers to establish multiple-hop TCP connections between them.*

Configuring the Way to Advertise/Receive Routing Information

Configuration Prerequisites

Make sure the following operation is performed before configuring the way to advertise/receive BGP routing information.

- Enabling the basic BGP functions

Make sure the following information is available when you configure the way to advertise/receive BGP routing information.

- The aggregation mode, and the aggregated route.
- Access list number
- Filtering direction (advertising/receiving) and the route policies to be adopted.
- Route dampening settings, such as half-life and the thresholds.

Importing Routes

With BGP employed, an AS can send its interior routing information to its neighbor ASs. However, the interior routing information is not generated by BGP, it is obtained by importing IGP routing information to BGP routing table. Once IGP routing information is imported to BGP routing table, it is advertised to BGP peers. You can filter IGP routing information by routing protocols before the IGP routing information is imported to BGP routing table.

Table 291 Import routes

Operation	Command	Description
Enter system view	**system-view**	-
Enable BGP, and enter BGP view	**bgp** *as-number*	Required
		By default, BGP is disabled.
Import and advertise routing information generated by other protocols.	**import-route** *protocol* [*process-id*] [**med** *med-value* | **route-policy** *route-policy-name*]*	Required
		By default, BGP does not import nor advertise the routing information generated by other protocols.
Advertise network segment routes to BGP routing table	**network** *network-address* [*mask*] [**route-policy** *route-policy-name*]	Optional
		By default, BGP does not advertise any network segment routes. Optional
		By default, BGP does not advertise any network segment routes. Optional
		By default, BGP does not advertise any network segment routes.

CAUTION:

- *If a route is imported to the BGP routing table through the **import-route** command, its Origin attribute is Incomplete.*
- *The network segment route to be advertised must be in the local IP routing table. You can use routing policy to control route advertising with more flexibility.*
- *The Origin attribute of the network segment routes advertised to BGP routing table through the **network** command is IGP.*

Configuring BGP Route Aggregation

In a medium-/large-sized BGP network, you can reduce the number of the routes to be advertised to BGP peers through route aggregation to save the spaces of BGP peer routing tables. BGP supports two route aggregation modes: automatic aggregation mode and manual aggregation mode.

- Automatic aggregation mode, where IGP sub-network routes imported by BGP are aggregated. In this mode, only the aggregated routes are advertised. The imported IGP sub-network routes are not advertised. Note that the default routes and the routes imported by using the **network** command cannot be automatically aggregated.
- Manual aggregation mode, where local BGP routes are aggregated. The priority of manual aggregation is higher than that of automatic aggregation.

Table 292 Configure BGP route aggregation

Operation		Command	Description
Enter system view		**system-view**	-
Enable BGP, and enter BGP view		**bgp** *as-number*	Required By default, BGP is disabled.
Configure BGP route aggregation	Enable automatic route aggregation	**summary**	Required By default, routes are not aggregated.
	Enable manual route aggregation	**aggregate** *ip-address mask* [**as-set** | **attribute-policy** *route-policy-name* | **detail-suppressed** | **origin-policy** *route-policy-name* | **suppress-policy** *route-policy-name*]*	

Enabling Default Route Advertising

Table 293 Enable default rout advertising

Operation	Command	Description
Enter system view	**system-view**	-
Enable BGP, and enter BGP view	**bgp** *as-number*	Required By default, BGP is disabled.
Enable default route advertising	**peer** *group-name* **default-route-advertise**	Required By default, a BGP router does not send default routes to a specified peer group.

*With the **peer default-route-advertise** command executed, no matter whether the default route is in the local routing table or not, a BGP router sends a default route, whose next hop address is the local address, to the specified peer or peer group.*

Configuring the BGP Route Advertising Policy

Table 294 Configure the BGP route advertising policy

Operation	Command	Description
Enter system view	**system-view**	-
Enable BGP, and enter BGP view	**bgp** *as-number*	Required By default, BGP is disabled.
Filter the advertised routes	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol* [*process-id*]]	Required By default, advertised routes are not filtered.
Specify a route advertising policy for the routes advertised to a peer group	**peer** *group-name* **route-policy** *route-policy-name* **export**	Required By default, no route advertising policy is specified for the routes advertised to a peer group.

Table 294 Configure the BGP route advertising policy

Operation		Command	Description
Filter the routing information to be advertised to a peer group	Specify an ACL-based BGP route filtering policy for a peer group	**peer** *group-name* **filter-policy** *acl-number* **export**	Required By default, a peer group has no peer group-based ACL BGP route filtering policy, AS path ACL-based BGP route filtering policy, or IP prefix list-based BGP route filtering policy configured.
	Specify an AS path ACL-based BGP filtering policy for a peer group	**peer** *group-name* **as-path-acl** *acl-number* **export**	
	IP prefix-based BGP route filtering policy for a peer group	**peer** *group-name* **ip-prefix** *ip-prefix-name* **export**	



CAUTION:

- *Only the routes that pass the specified filter are advertised.*
- *A peer group member uses the same outbound route filtering policy as that of the peer group it belongs to. That is, a peer group adopts the same outbound route filtering policy.*

Configuring BGP Route Receiving Policy

Table 295 Configure BGP route receiving policy

Operation	Command	Description
Enter system view	**system-view**	-
Enable BGP, and enter BGP view	**bgp** *as-number*	Required By default, BGP is disabled.
Filter the received global routing information	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **import**	Required By default, the received routing information is not filtered.
Specify a route filtering policy for routes coming from a peer/peer group	**peer** { *group-name* | *ip-address* } **route-policy** *policy-name* **import**	Required By default, no route filtering policy is specified for a peer/peer group.

Table 295 Configure BGP route receiving policy

Operation		Command	Description
Filter the routing information received from a peer/peer group	Specify an ACL-based BGP route filtering policy for a peer/peer group	**peer** { *group-name* | *ip-address* } **filter-policy** *acl-number* **import**	Required By default, no ACL-based BGP route filtering policy, AS path ACL-based BGP route filtering policy, or IP prefix list-based BGP route filtering policy is configured for a peer/peer group.
	Specify an AS path ACL-based BGP route filtering policy for a peer/peer group	**peer** { *group-name* | *ip-address* } **as-path-acl** *acl-number* **import**	
	Specify an IP prefix list-based BGP route filtering policy for a peer/peer group	**peer** { *group-name* | *ip-address* } **ip-prefix** *ip-prefix-name* **import**	

Configuring BGP-IGP Route Synchronization

Table 296 Configure BGP-IGP route synchronization

Operation	Command	Description
Enter system view	**system-view**	-
Enable BGP, and enter BGP view	**bgp** *as-number*	Required By default, BGP is disabled.
Disable BGP-IGP route synchronization	undo synchronization	Required By default, BGP routes and IGP routes are not synchronized.



CAUTION: *BGP-IGP route synchronization is not supported on Switch 7750 Ethernet switches.*

Configuring BGP Route Dampening

Route dampening is used to solve the problem of route instability. Route instability mainly refers to route flapping. A route flaps if it appears and disappears repeatedly in the routing table. Route flapping increases the number of BGP update packets, consumes the bandwidth and CPU time, and even decreases network performance.

Assessing the stability of a route is based on the behavior of the route in the previous time. Once a route flaps, it receives a certain penalty value. When the penalty value reaches the suppression threshold, this route is suppressed. The penalty value decreases with time. When the penalty value of a suppressed route decreases to the reuse threshold, the route gets valid and is thus advertised again.

BGP dampening suppresses unstable routing information. Suppressed routes are neither added to the routing table nor advertised to other BGP peers.

Table 297 Configure BGP route dampening

Operation	Command	Description
Enter system view	**system-view**	-
Enable BGP, and enter BGP view	**bgp** *as-number*	Required By default, BGP is disabled.
Configure BGP route dampening-related parameters	**dampening** [*half-life-reachable half-life-unreachable reuse suppress ceiling*] [**route-policy** *route-policy-name*]	Optional By default, route dampening is disabled. Other default route dampening-related parameters are as follows. ■ *half-life-reachable*: 15 (in minutes) ■ *half-life-unreachable*: 15 (in minutes) ■ *reuse*: 750 ■ *suppress*: 2000 ■ *ceiling*: 16,000

Configuring BGP Load Balance

Table 298 Configure BGP load balance

Operation	Command	Description
Enter system view	**system-view**	-
Enable BGP and enter BGP view	**bgp** as-number	-
Configure BGP load balance	**balance** *num*	Required By default, the system does not adopt BGP load balance.

Configuring BGP Route Attributes

Configuring BGP Route Attributes

BGP possesses many route attributes for you to control BGP routing policies.

Table 299 Configure BGP route attributes

Operation	Command	Description
Enter system view	**system-view**	-
Enable BGP, and enter BGP view	**bgp** *as-number*	Required By default, BGP is disabled.
Configure the management preference of the exterior, interior and local routes	**preference** { *ebgp-value ibgp-value local-value* }	Optional By default, the management preference of the exterior, interior and local routes is 256, 256, and 130.
Set the default local preference	**default local-preference** *value*	Optional By default, the local preference defaults to 100.

Table 299 Configure BGP route attributes

Operation		Command	Description
Configure the MED attribute	Configure the default local MED value	**default med** *med-value*	Optional By default, the *med-value* argument is 0.
	Permit to compare the MED values of the routes coming from the neighbor routers in different ASs.	**compare-different-as-med**	Optional By default, the compare of MED values of the routes coming from the neighbor routers in different ASs is disabled.
Configure the local address as the next hop address when a BGP router advertises a route.		**peer** *group-name* **next-hop-local**	Required In some network, to ensure an IBGP neighbor locates the correct next hop, you can configure the next hop address of a route to be the local address for a BGP router to advertise route information to IBGP peer groups.
Configure the AS_Path attribute	Configure the number of local AS number occurrences allowed	**peer** { *group-name* | *ip-address* } **allow-as-loop** [*number*]	Optional By default, the number of local AS number occurrences allowed is 1.
	Assign an AS number for a peer group	**peer** *group-name* **as-number** *as-number*	Optional By default, the local AS number is not assigned to a peer group.
	Configure that the BGP update packets only carry the pubic AS number in the AS_Path attribute when a peer sends BGP update packets to BGP peers.	**peer** *group-name* **public-as-only**	Optional By default, a BGP update packet carries the private AS number.



CAUTION:

- *Using routing policy, you can configure the preference for the routes that match the filtering conditions. As for the unmatched routes, the default preference is adopted.*
- *If other conditions are the same, the route with the lowest MED value is preferred to be the exterior route of the AS.*
- *After BGP load balance is configured, no matter whether the **peer next-hop-local** command is executed or not, the local router changes the next hop IP address to its own IP address before advertising a route to its IBGP peers/peer group.*

Adjusting and Optimizing a BGP Network

Adjusting and optimizing BGP network involves the following aspects:

1 BGP clock

BGP peers send Keepalive messages to each other periodically through the connections between them to make sure the connections operate properly. If a router does not receive the Keepalive or any other message from its peer in a specific period (know as Holdtime), the router considers the BGP connection operates improperly and thus disconnects the BGP connection.

When establishing a BGP connection, the two routers negotiate for the Holdtime by comparing their Holdtime values and take the smaller one as the Holdtime.

2 Limiting the number of route prefixes to be received from the peer/peer group

By limiting the number of route prefixes to be received from the specified peer/peer group, you can control the size of the local routing table, thus optimizing the performance of local router system and protecting local routers.

When the number of route prefixes received exceeds the configured value, a router enabled with this function is automatically disconnected from the peer/peer group.

3 BGP connection reset

To make a new BGP routing policy taking effect, you need to reset the BGP connection. This temporarily disconnects the BGP connection. In the Switch 7750, BGP supports the route-refresh function. With route-refresh function enabled on all the BGP routers, if BGP routing policy changes, the local router sends refresh messages to its peers. And the peers receiving the message in turn send their routing information to the local router. In this way, you can apply new routing policies and have the routing table dynamically updated seamlessly.

Use the **refresh bgp** command to reset the BGP connections manually. This method can also refresh BGP routing tables and apply a new routing policy seamlessly.

4 BGP authentication

BGP uses TCP as the transport layer protocol. To improve the security of BGP connections, you can specify to perform MD5 authentication when a TCP connection is established. Note that the MD5 authentication of BGP does not authenticate the BGP packets. It only configures the MD5 authentication password for TCP connection, and the authentication is performed by TCP. If authentication fails, the TCP connection cannot be established.

Configuration Prerequisites

You need to perform the following configuration before adjusting the BGP clock.

- Enable basic BGP functions

Before configuring BGP clock and authentication, make sure the following information is available.

- Value of BGP timer
- Interval for sending the update packets
- MD5 authentication password

Adjusting and Optimizing a BGP Network

Table 300 Adjust and optimize a BGP network

Operation		Command	Description
Enter system view		**system-view**	-
Enable BGP, and enter BGP view		**bgp** *as-number*	Required By default, BGP is disabled.
Configure BGP timer	Configure the Keepalive time and Holdtime of BGP.	**timer keepalive** *keepalive-interval* **hold** *holdtime-interval*	Optional By default, the keepalive time is 60 seconds, and holdtime is 180 seconds. The priority of the timer configured by the **timer** command is lower than that of the timer configured by the **peer time** command.
	Configure the Keepalive time and holdtime of a specified peer/peer group.	**peer** { *group-name* | *ip-address* } **timer keepalive** *keepalive-interval* **hold** *holdtime-interval*	
Configure the interval at which a peer group sends the same route update packet		**peer** *group-name* **route-update-interval** *seconds*	Optional By default, the interval at which a peer group sends the same route update packet to IBGP peers is 15 seconds, and to EBGP peers is 30 seconds.
Configure the number of route prefixes to be received from the BGP peer/peer group		**peer** { *group-name* | *ip-address* } **route-limit** *prefix-number* [[**alert-only** | **reconnect** *reconnect-time*] | *percentage-value*] *	Optional By default, there is no limit on the number of route prefixes to be received from the BGP peer/peer group.
Perform soft refreshment of BGP connection manually		**return**	-
		refresh bgp { **all** | *ip-address* | **group** *group-name* } { **export** | **import** }	Optional
		system-view	Enter BGP view again
		bgp *as-number*	
Configure BGP to perform MD5 authentication when establishing TCP connection		**peer** { *group-name* | *ip-address* } **password** { **cipher** | **simple** } *password*	Optional By default, BGP dose not perform MD5 authentication when establishing TCP connection.
Configure the number of routes used for BGP load balance		**balance** *num*	Optional By default, the system does not adopt BGP load balance.

CAUTION:

- *The reasonable maximum interval for sending Keepalive message is one third of the Holdtime, and the interval cannot be less than 1 second, therefore, if the Holdtime is not 0, it must be 3 seconds at least.*

- *BGP soft reset can refresh the BGP routing table and apply a new routing policy without breaking the NGP connections.*

Configuring a Large-Scale BGP Network

In large-scale network, there are large quantities of peers. Configuring and maintaining the peer becomes a big problem. Using peer group can ease the management and improve the routes sending efficiency. According to the different ASs where peers reside, the peer groups fall into IBGP peer groups and EBGP peer groups. For the EBGP peer group, it can also be divided into pure EBGP peer group and hybrid EBGP peer group according to whether the peers in the EBGP group belong to the same exterior AS or not.

Community can also be used to ease the routing policy management. And its management range is much wider than that of the peer group. It controls the routing policy of multiple BGP routers.

In an AS, to ensure the connectivity among IBGP peers, you need to set up full connection among them. When there are too many IBGP peers, it will cost a lot in establishing a full connection network. Using RR or confederation can solve the problem. In a large AS, RR and confederation can be used simultaneously.

Configuration Prerequisites

Before configuring a large-scale BGP network, you need to ensure:

- Network layer connectivity between adjacent nodes.

Before configuring a large-scale BGP network, you need to prepare the following data:

- Peer group type, name, and the peers included.
- If you want to use community, the name of the applied routing policy is needed.
- If you want to use RR, you need to determine the roles (client, non-client) of routers.
- If you want to use confederation, you need to determine the confederation ID and the sub-AS number.

Configuring BGP Peer Group

Table 301 Configure BGP peer group

Operation	Command	Description
Enter system view	**system-view**	-
Enable BGP, and enter BGP view	**bgp** *as-number*	Required By default, the system does not operate BGP.

Table 301 Configure BGP peer group

Operation		Command	Description
Create an IBGP peer group	Create an IBGP peer group	**group** *group-name* [**internal**]	Optional If the command is executed without the **internal** or **external** keyword, an IBGP peer group will be created. You can add multiple peers to the group, and the system will automatically create a peer in BGP view, and configure its AS number as the local AS number.
	Add a peer to a peer group	**peer** *ip-address* **group** *group-name* [**as-number** *as-number*]	
Create an EBGP peer group	Create an EBGP peer group	**group** *group-name* **external**	Optional You can add multiple peers to the group. The system automatically creates the peer in BGP view and specifies its AS number as the one of the peer group.
	Configure the AS number of a peer group	**peer** *group-name* **as-number** *as-number*	

CAUTION:

- *It is not required to specify an AS number for creating an IBGP peer group.*
- *If there already exists a peer in a peer group, you can neither change the AS number of the peer group, nor delete a specified AS number through the* ***undo*** *command.*

Configuring BGP Community

Table 302 Configure BGP community

Operation	Command	Description
Enter system view	**system-view**	-
Enable BGP, and enter BGP view	**bgp** *as-number*	Required By default, the system does not operate BGP.
Configure the peers to advertise community attribute to the peer group	**peer** *group-name* **advertise-community**	Required By default, no community attribute or extended community attribute is advertised to any peer group.
Specify routing policy for the routes exported to the peer group	**peer** *group-name* **route-policy** *route-policy-name* **export**	Required By default, no routing policy is specified for the routes exported to the peer group.

CAUTION:

- *When configuring BGP community, you must use a routing policy to define the specific community attribute, and then apply the routing policy when a peer sends routing information.*
- *For configuration of routing policy, refer to "IP Routing Policy Configuration" on page 378.*

Configuring BGP RR

Table 303 Configure BGP RR

Operation	Command	Description
Enter system view	**system-view**	-
Enable BGP, and enter BGP view	**bgp** *as-number*	Required By default, the system does not operate BGP.
Configure the local router as the RR and configure the peer group as the client of the RR	**peer** *group-name* **reflect-client**	Required By default, no RR and its client is configured.
Enable route reflection between clients	**reflect between-clients**	Optional By default, route reflection is enabled between clients.
Configure cluster ID of an RR	**reflector cluster-id** *cluster-id*	Optional By default, an RR uses its own router ID as the cluster ID.

CAUTION:

- *Normally, full connection is not required between an RR and a client. A route is reflected by an RR from a client to another client. If an RR and a client are fully connected, you can disable the reflection between clients to reduce the cost.*
- *Normally, there is only one RR in a cluster. In this case, the router ID of the RR is used to identify the cluster. Configuring multiple RRs can improve the network stability. If there are multiple RRs in a cluster, use related command to configure the same cluster ID for them to avoid routing loops.*

Configuring BGP Confederation

Table 304 Configure BGP confederation

Operation		Command	Description
Enter system view		**system-view**	-
Enable BGP, and enter BGP view		**bgp** *as-number*	Required By default, the system does not operate BGP.
Basic BGP confederation configuration	Configure confederation ID	**confederation id** *as-number*	Required By default, no confederation ID is configured and no sub-AS is configured for a confederation.
	Specify the sub-ASs included in a confederation	**confederation peer-as** *as-number-list*	
Configure the compatibility of a confederation		**confederation nonstandard**	Optional By default, the confederation configured is consistent with the RFC1965.

CAUTION:

- *A confederation can include up to 32 sub-ASs. The AS number used by a sub-AS which is configured to belong to a confederation is only valid inside the confederation.*

- *If the confederation implementation mechanism of other routers is different from the RFC standardization, you can configure related command to make the confederation compatible with the non-standard routers.*

Displaying and maintaining BGP

Displaying BGP

After the above configuration, you can use the **display** command in any view to display the BGP configuration and thus verify the configuration effect.

Table 305 Display BGP

Operation	Command
Display information about peer group	**display** bgp [**multicast**] **group** [*group-name*]
Display routing information exported by BGP	**display bgp** [**multicast**] **network**
Display information about AS path	**display bgp paths** [*as-regular-expression*]
Display information about a BGP peer	**display bgp** [**multicast**] **peer** [*ip-address* [**verbose**]]
	display bgp [**multicast**] **peer** [**verbose**]
Display information in the BGP routing table	**display bgp** [**multicast**] **routing-table** [*ip-address* [*mask*]]
Display the route matching with the specific AS path ACL.	**display bgp** [**multicast**] **routing-table as-path-acl** *acl-number*
Display routing information about CIDR	**display bgp** [**multicast**] **routing-table cidr**
Display routing information about a specified BGP community.	**display bgp** [**multicast**] **routing-table community** [*aa:nn* | **no-export-subconfed** | **no-advertise** | **no-export**]* [**whole-match**]
Display the route matching with the specific BGP community ACL.	**display bgp** [**multicast**] **routing-table community-list** *community-list-number* [**whole-match**]
Display information about BGP route dampening	**display bgp routing-table dampened**
Display routes with different source ASs	**display bgp** [**multicast**] **routing-table different-origin-as**
Display statistic information about route flaps.	**display bgp routing-table flap-info** [**regular-expression** *as-regular-expression* | **as-path-acl** *acl-number* | *network-address* [*mask* [**longer-match**]]]
Display routing information sent to or received from a specific BGP peer	**display bgp** [**multicast**] **routing-table peer** *ip-address* { **advertised-routes** | **received-routes** } [*network-address* [*mask*] | **statistic**]
Display routing information matching with the AS regular expression	**display bgp** [**multicast**] **routing-table regular-expression** *as-regular-expression*
Display routing statistics of BGP	**display bgp** [**multicast**] **routing-table statistic**

BGP Connection Reset

When a BGP routing policy or protocol changes, if you need to make the new configuration effective through resetting the BGP connection, perform the following configuration in user view.

Table 306 Reset BGP connection

Operation	Command
Reset all BGP connections	**reset bgp all**
Reset the BGP connection with a specified peer	**reset bgp** *ip-address*
Reset the BGP connection with a specified peer group	**reset bgp group** *group-name*

Clearing BGP Information

Use the **reset** command in user view to clear the related BGP statistic information.

Table 307 Clear BGP information

Operation	Command
Clear the route dampening information and release the suppressed routes	**reset bgp dampening** [*network-address* [*mask*]]
Clear the route flaps statistics	**reset bgp flap-info** [**regular-expression** *as-regular-expression* | **as-path-acl** *acl-number* | *ip-address* [*mask*]]

Configuration Example

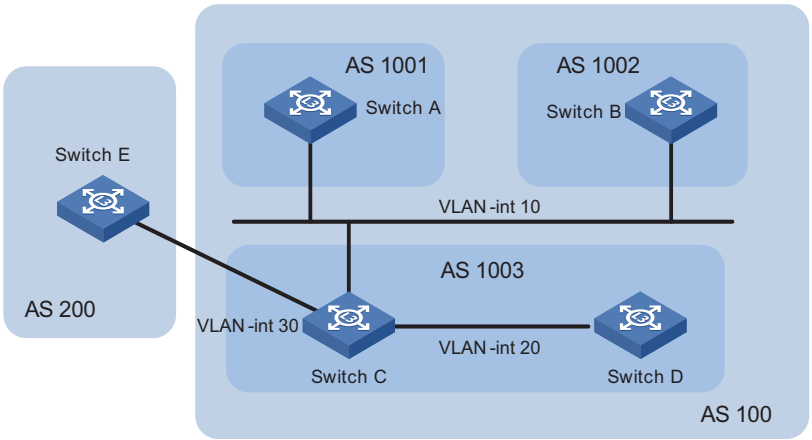
Configuring BGP AS Confederation Attribute

Network requirements

Divide the AS 100 shown in the following figure into three sub-ASs: 1001, 1002, and 1003. Configure EBGP, Confederation EBGP, and IBGP.

Network diagram

Figure 84 Diagram for AS confederation



Device	Interface	IP address	AS

Switch A	Vlan-int 10	172.68.10.1/24	100
Switch B	Vlan-int 10	172.68.10.2/24	
Switch C	Vlan-int 10	172.68.10.3/24	
	Vlan-int 20	172.68.1.1/24	
	Vlan-int 30	156.10.1.1/24	
Switch D	Vlan-int 20	172.68.1.2/24	
Switch E	Vlan-int 30	156.10.1.2/24	200

Configuration procedure

Configure SwitchA.

```
[SwitchA] bgp 1001
[SwitchA-bgp] confederation id 100
[SwitchA-bgp] confederation peer-as 1002 1003
[SwitchA-bgp] group confed1002 external
[SwitchA-bgp] peer 172.68.10.2 group confed1002 as-number 1002
[SwitchA-bgp] group confed1003 external
[SwitchA-bgp] peer 172.68.10.3 group confed1003 as-number 1003
```

Configure SwitchB.

```
[SwitchB] bgp 1002
[SwitchB-bgp] confederation id 100
[SwitchB-bgp] confederation peer-as 1001 1003
[SwitchB-bgp] group confed1001 external
[SwitchB-bgp] peer 172.68.10.1 group confed1001 as-number 1001
[SwitchB-bgp] group confed1003 external
[SwitchB-bgp] peer 172.68.10.3 group confed1003 as-number 1003
```

Configure SwitchC.

```
[SwitchC] bgp 1003
[SwitchC-bgp] confederation id 100
[SwitchC-bgp] confederation peer-as 1001 1002
[SwitchC-bgp] group confed1001 external
[SwitchC-bgp] peer 172.68.10.1 group confed1001 as-number 1001
[SwitchC-bgp] group confed1002 external
[SwitchC-bgp] peer 172.68.10.2 group confed1002 as-number 1002
[SwitchC-bgp] group ebgp200 external
[SwitchC-bgp] peer 156.10.1.2 group ebgp200 as-number 200
[SwitchC-bgp] group ibgp1003 internal
[SwitchC-bgp] peer 172.68.1.2 group ibgp1003
```

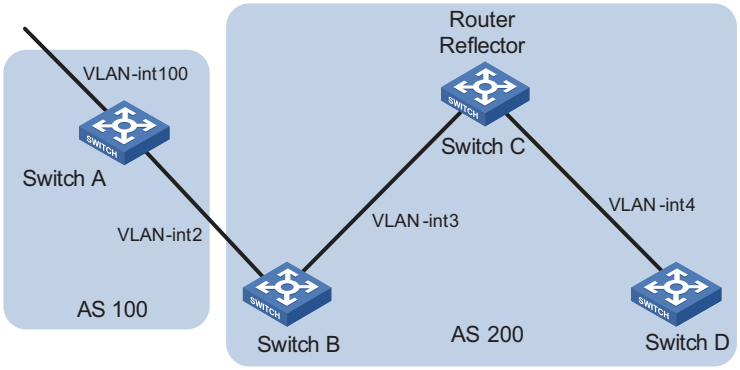
Configuring BGP RR

Network requirements

SwitchB receives an update packet passing through the EBGP, and transfers the packet to SwitchC. SwitchC is configured as an RR with two clients SwitchB and SwitchD. After SwitchC receives the routing update information, it reflects the message to SwitchD. You need not to establish IBGP connection between SwitchB and SwitchD, because SwitchC reflects information from SwitchC to SwitchD.

Network diagram

Figure 85 Diagram for configuring a BGP RR



Device	Interface	IP address	AS
Switch A	Vlan-int 100	1.1.1.1/8	100
	Vlan-int 2	192.1.1.1/24	
Switch B	Vlan-int 2	192.1.1.2/24	200
	Vlan-int 3	193.1.1.2/24	
Switch C	Vlan-int 3	193.1.1.1/24	
	Vlan-int 4	194.1.1.1/24	
Switch D	Vlan-int 4	194.1.1.2/24	

Configuration procedure

1 Configure SwitchA.

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] ip address 192.1.1.1 255.255.255.0
[SwitchA-Vlan-interface2] interface Vlan-interface 100
[SwitchA-Vlan-interface100] ip address 1.1.1.1 255.0.0.0
[SwitchA-Vlan-interface100] quit
[SwitchA] bgp 100
[SwitchA-bgp] group ex external
[SwitchA-bgp] peer 192.1.1.2 group ex as-number 200
[SwitchA-bgp] network 1.0.0.0 255.0.0.0
```

2 Configure SwitchB.

Configure VLAN2.

```
[SwitchB] interface Vlan-interface 2
[SwitchB-Vlan-interface2] ip address 192.1.1.2 255.255.255.0
```

Configure VLAN3.

```
[SwitchB] interface Vlan-interface 3
[SwitchB-Vlan-interface3] ip address 193.1.1.2 255.255.255.0
```

Configure a BGP peer.

```
[SwitchB] bgp 200
[SwitchB-bgp] group ex external
[SwitchB-bgp] peer 192.1.1.1 group ex as-number 100
```

```
[SwitchB-bgp] group in internal
[SwitchB-bgp] peer 193.1.1.1 group in
```

3 Configure SwitchC.

Configure VLAN3.

```
[SwitchC] interface Vlan-interface 3
[SwitchC-Vlan-interface3] ip address 193.1.1.1 255.255.255.0
```

Configure VLAN4.

```
[SwitchC] interface vlan-Interface 4
[SwitchC-Vlan-interface4] ip address 194.1.1.1 255.255.255.0
```

Configure BGP peers and RR.

```
[SwitchC] bgp 200
[SwitchC-bgp] group rr internal
[SwitchC-bgp] peer rr reflect-client
[SwitchC-bgp] peer 193.1.1.2 group rr
[SwitchC-bgp] peer 194.1.1.2 group rr
```

4 Configure SwitchD.

Configure VLAN4.

```
[SwitchD] interface vlan-interface 4
[SwitchD-Vlan-interface4] ip address 194.1.1.2 255.255.255.0
```

Configure a BGP peer.

```
[SwitchD] bgp 200
[SwitchD-bgp] group in internal
[SwitchD-bgp] peer 194.1.1.1 group in
```

Use the **display bgp routing-table** command to display the BGP routing table on SwitchB. Note that, SwitchB has already known the existence of network 1.0.0.0.

Use the **display bgp routing-table** command to display the BGP routing table on SwitchD. Note that, SwitchD knows the existence of network 1.0.0.0, too.

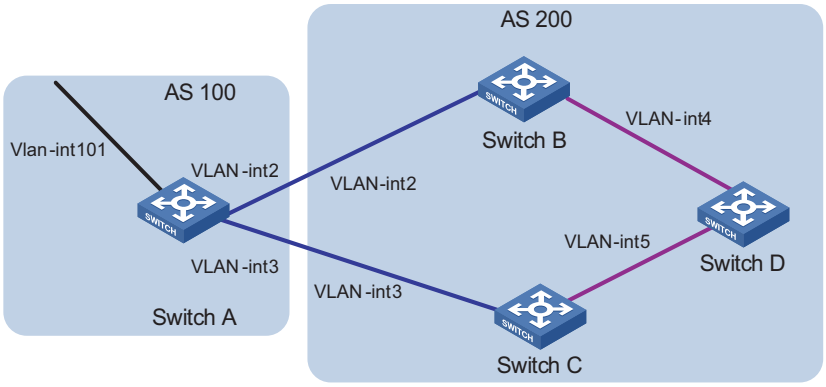
Configuring BGP Routing

Network requirements

BGP is applied to all switches, and OSPF is applied to the IGP in AS200. SwitchA is in AS100, and SwitchB, SwitchC, and SwitchD are in AS200. EBGP is running between SwitchA and SwitchB, and between SwitchA and SwitchC. IBGP is running between SwitchB and SwitchC, and between SwitchB and SwitchD.

Network diagram

Figure 86 Diagram for BGP routing



Device	Interface	IP address	AS
Switch A	Vlan-int 101	1.1.1.1/8	100
	Vlan-int 2	192.1.1.1/24	
	Vlan-int 3	193.1.1.1/24	
Switch B	Vlan-int 2	192.1.1.2/24	200
	Vlan-int 4	194.1.1.2/24	
Switch C	Vlan-int 3	193.1.1.2/24	
	Vlan-int 5	195.1.1.2/24	
Switch D	Vlan-int 4	194.1.1.1/24	
	Vlan-int 5	195.1.1.1/24	

Configuration procedure

1 Configure Switch A.

```
[SwitchA] interface Vlan-interface 2
[SwitchA-Vlan-interface2] ip address 192.1.1.1 255.255.255.0
[SwitchA] interface Vlan-interface 3
[SwitchA-Vlan-interface3] ip address 193.1.1.1 255.255.255.0
```

Enable BGP

```
[SwitchA] bgp 100
```

Specify the destination network for BGP routes.

```
[SwitchA-bgp] network 1.0.0.0
```

Configure BGP peers.

```
[SwitchA-bgp] group ex192 external
[SwitchA-bgp] peer 192.1.1.2 group ex192 as-number 200
[SwitchA-bgp] group ex193 external
[SwitchA-bgp] peer 193.1.1.2 group ex193 as-number 200
[SwitchA-bgp] quit
```

Configure the MED attribute of Switch A.

Create an access control list to permit routing information sourced from the network 1.0.0.0.

```
[SwitchA] acl number 2000
[SwitchA-acl-basic-2000] rule permit source 1.0.0.0 0.255.255.255
[SwitchA-acl-basic-2000] rule deny source any
```

Define two routing policies, named apply_med_50 and apply_med_100 respectively. The first routing policy apply_med_50 configures the MED attribute as 50 for network 1.0.0.0, and the second one apply_med_100 configures the MED attribute for the network as 100.

```
[SwitchA] route-policy apply_med_50 permit node 10
[SwitchA-route-policy] if-match acl 2000
[SwitchA-route-policy] apply cost 50
[SwitchA-route-policy] quit
[SwitchA] route-policy apply_med_100 permit node 10
[SwitchA-route-policy] if-match acl 2000
[SwitchA-route-policy] apply cost 100
[SwitchA-route-policy] quit
```

Apply apply_med_50 to the outbound routing update of neighbor Switch C (193.1.1.2), and apply apply_med_100 to the outbound routing update of neighbor Switch B (192.1.1.2).

```
[SwitchA] bgp 100
[SwitchA-bgp] peer ex193 route-policy apply_med_50 export
[SwitchA-bgp] peer ex192 route-policy apply_med_100 export
```

2 Configure Switch B.

```
[SwitchB] interface vlan 2
[SwitchB-Vlan-interface2] ip address 192.1.1.2 255.255.255.0
[SwitchB] interface vlan-interface 4
[SwitchB-Vlan-interface4] ip address 194.1.1.2 255.255.255.0
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 194.1.1.0 0.0.0.255
[SwitchB-ospf-1-area-0.0.0.0] network 192.1.1.0 0.0.0.255
[SwitchB] bgp 200
[SwitchB-bgp] undo synchronization
[SwitchB-bgp] group ex external
[SwitchB-bgp] peer 192.1.1.1 group ex as-number 100
[SwitchB-bgp] group in internal
[SwitchB-bgp] peer 194.1.1.1 group in
[SwitchB-bgp] peer 195.1.1.2 group in
```

3 Configure Switch C.

```
[SwitchC] interface Vlan-interface 3
[SwitchC-Vlan-interface3] ip address 193.1.1.2 255.255.255.0
[SwitchC] interface vlan-interface 5
[SwitchC-Vlan-interface5] ip address 195.1.1.2 255.255.255.0
[SwitchC] ospf
[SwitchC-ospf-1] area 0
[SwitchC-ospf-1-area-0.0.0.0] network 193.1.1.0 0.0.0.255
[SwitchC-ospf-1-area-0.0.0.0] network 195.1.1.0 0.0.0.255
[SwitchC] bgp 200
[SwitchC-bgp] undo synchronization
```

```
[SwitchC-bgp] group ex external
[SwitchC-bgp] peer 193.1.1.1 group ex as-number 100
[SwitchC-bgp] group in internal
[SwitchC-bgp] peer 195.1.1.1 group in
[SwitchC-bgp] peer 194.1.1.2 group in
```

4 Configure Switch D.

```
[SwitchD] interface vlan-interface 4
[SwitchD-Vlan-interface4] ip address 194.1.1.1 255.255.255.0
[SwitchD] interface vlan-interface 5
[SwitchD-Vlan-interface5] ip address 195.1.1.1 255.255.255.0
[SwitchD] ospf
[SwitchD-ospf-1] area 0
[SwitchD-ospf-1-area-0.0.0.0] network 194.1.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] network 195.1.1.0 0.0.0.255
[SwitchD-ospf-1-area-0.0.0.0] network 4.0.0.0 0.255.255.255
[SwitchD] bgp 200
[SwitchD-bgp] undo synchronization
[SwitchD-bgp] group in internal
[SwitchD-bgp] peer 195.1.1.2 group in
[SwitchD-bgp] peer 194.1.1.2 group in
```

- To make the configuration take effect, all BGP neighbors need to execute the **reset bgp all** command.
- After the above configuration, because the MED attribute value of the route 1.0.0.0 learnt by Switch C is smaller than that of the route 1.0.0.0 learnt by Switch B, Switch D will choose the route 1.0.0.0 coming from Switch C.
- If you do not configure MED attribute of Switch A when you configure Switch A, but configure the local preference on Switch C as following:

Configure the local preference of Switch C

- Create ACL 2000 to permit routing information sourced from network 1.0.0.0.

```
[SwitchC] acl number 2000
[SwitchC-acl-basic-2000] rule permit source 1.0.0.0 0.255.255.255
[SwitchC-acl-basic-2000] rule deny source any
```

- Define a routing policy named localpref, and set the local preference of the routes matching with ACL 2000 to 200, and that of those unmatched routes to 100.

```
[SwitchC] route-policy localpref  permit node 10
[SwitchC-route-policy] if-match acl 2000
[SwitchC-route-policy] apply local-preference 200
[SwitchC-route-policy] quit
[SwitchC] route-policy localpref permit node 20
[SwitchC-route-policy] apply local-preference 100
[SwitchC-route-policy] quit
```

- Apply this routing policy to the inbound traffic flows coming from BGP neighbor 193.1.1.1 (Switch A).

```
[SwitchC] bgp 200
[SwitchC-bgp] peer 193.1.1.1 route-policy localpref import
```

In this case, because the local preference value of the route 1.0.0.0 learnt by Switch C is 200, which is greater than that of the route 1.0.0.0 learnt by Switch B

(Switch B does not configure the local preference attribute, the default value is 100), Switch D still chooses the route 1.0.0.0 coming from Switch C first.

BGP Error Configuration Example

BGP Peer Connection Establishment Error

Symptom 1: A BGP neighbor relationship cannot be established, that is the connection with the opposite peer cannot be established.

Solution: The BGP neighbor establishment process requires using port 179 to establish a TCP session and exchanging Open messages correctly. You can follow these steps to solve the problem:

- Check the AS number of the neighbor.
- Check the IP address of the neighbor.
- Use the **ping** command to check the TCP connection. As a router may have more than one interface to reach the peer, you should use the **ping -a** *ip-address* expanded command to specify a source IP address for sending ping packets.
- If you cannot ping through the neighbor device, check whether there is a route to the neighbor in the routing table.
- If you can ping through the neighbor device, check whether an ACL is configured to inhibit TCP port 179. If yes, cancel the inhibition of port 179.

Symptom 2: After you use the **network** command to import the routes discovered by IGP to BGP, the BGP routes cannot be successfully advertised.

Solution: For a route to be successfully imported into BGP, it is required that the route (including the destination network segment and mask) must not be conflict with any route in the routing table. For example, a route to the network segment 10.1.1.0/24 exists in the routing table, if a route to 10.0.0.0/8 or other similar segment is imported, an import error will occur. If OSPF is used, when you use the **network** command to import a bigger network segment, the router will change the route according to the actual interface network segment. This may result in unsuccessful route import or wrong import, and may cause routing error in some network trouble situations.

37 IP ROUTING POLICY CONFIGURATION

IP Routing Policy Overview

When a router distributes or receives routing information, it may need to implement some policies to filter the routing information, so as to receive or distribute only the routing information meeting given conditions. A routing protocol (RIP, for example) may need to import the routing information discovered by other protocols to enrich its routing knowledge. While importing routing information from another protocol, it possibly only needs to import the routes meeting given conditions and set some attributes of the imported routes to make the routes meet the requirements of this protocol.

For the implementation of a routing policy, you need to define a set of matching rules by specifying the characteristics of the routing information to be filtered. You can set the rules based on such attributes as destination address and source address of the information. The matching rules can be set in advance and then used in the routing policies to advertise, receive, and import routes.

Filters

The Switch 7750 provide five kinds of filters (route-policy, ACL, AS-path, community-list and ip-prefix) that can be referenced by routing protocols. The following sections describe these filters.

Route-policy

A route-policy is used to match some attributes with given routing information and the attributes of the information will be set if the conditions are satisfied.

A route policy can comprise multiple nodes. Each node is a unit for matching test, and the nodes will be matched in the order of their node numbers. Each node comprises a set of **if-match** and **apply** statements. The **if-match** statements define the matching rules. The matching objects are some attributes of routing information. The relationship among the **if-match** statements for a node is "AND". As a result, a matching test against a node is successful only when all the matching conditions specified by the **if-match** statements in the node are satisfied. The **apply** statements specify the actions performed after a matching test against the node is successful, and the actions can be the attribute settings of routing information.

The relationships among different nodes in a route-policy are "OR". As a result, the system examines the nodes in the route-policy in sequence, and once the route passes a node in the route-policy, it will pass the matching test of the route-policy without entering the test of the next node.

ACL

Normally, a basic ACL is used to filter routing information. You can specify a range of IP addresses or subnets when defining a basic ACL so as to match the

destination network segment addresses or next-hop addresses of routing information. If an advanced ACL is used, the specified range of source addresses will be used for matching.

ip-prefix

ip-prefix plays a role similar to ACL. But it is more flexible than ACL and easier to understand. When ip-prefix is applied to filtering routing information, its matching object is the destination address information field of routing information.

An ip-prefix is identified by its ip-prefix name. Each ip-prefix can include multiple items, and each item, identified by an index-number, can independently specify the match range in network prefix form. An index-number specifies the matching sequence in the ip-prefix.

During the matching, the router checks items identified by index-number in ascending order. Once an item is met, the ip-prefix filtering is passed and no other item will be checked.

as-path

as-path is an access control list of autonomous system path. It is only used in BGP to define the matching conditions about AS path. An as-path contains a series of AS paths which are the records of routing information passed paths during BGP routing information exchange.

community-list

community-list is only used to define the matching conditions about community attributes in BGP. A BGP routing information packet contains a community attribute field used to identify a community.

Applications of Routing Policy

The following are main applications of routing policy:

- When a routing protocol advertises or receives routing information, it adopts routing policy to filter the routing information, so as to receive or advertise only the routing information meeting given conditions.
- When a routing protocol imports the routes discovered by other protocols into itself, it adopts routing policy to import only those routes meeting given conditions.

In addition, routing policy can also be used to change some route attributes.

IP Routing Policy Configuration

The configuration of routing policy includes the configuration of filters and the application of routing policy.

1 You can configure the following filters:

- Route-policy
- ACL
- IP prefix list
- AS path list
- Community attribute list



Refer to "ACL Configuration" on page 637.

2 You can have routing policy applied in the following cases:

- When routes are imported
- When routes are advertised/received

Configuring a Route-Policy

A route-policy can comprise multiple nodes. Each node is a unit for matching test, and the nodes will be matched in the order of their sequence numbers.

Each node comprises a set of **if-match** and **apply** clauses.

- The **if-match** clauses define the matching rules. The relationship among the **if-match** clauses in a node is logical "AND". That is, a matching test against a node is successful only when all the matching conditions specified by the **if-match** clauses in the node are satisfied.
- The **apply** clauses specify the actions performed after a matching test against the node is successful, and the actions can be the setting of route attributes.

Defining a route-policy

Table 308 Define a route-policy

Operation	Command	Description
Enter system view	**system-view**	-
Define a route-policy and enter the route-policy view	**route-policy** *route-policy-name* { **permit** | **deny** } **node** *node-number*	Required

The **permit** argument specifies that the matching mode for the defined node in the route-policy is "permit". In this mode, if a route matches all the **if-match** clauses of the node, the system considers that the route passes the filter of the node and then executes the **apply** clauses of the node and does not take the test of the next node. If not, the system goes on the test of the next node.

The **deny** argument specifies that the matching mode for the defined node in the route-policy is "deny". In this mode, no **apply** clause is executed. If a route satisfies all the **if-match** clauses of the node, the system considers that the route fails to pass through the node and does not take the test of the next node. If not, the system goes on the test of the next node.

The relationships among different nodes in a route-policy are logical "OR". As a result, the system examines the nodes in the route-policy in sequence for a route, and once the route passes a node in the route-policy, it passes the filter of the whole route-policy without going on the test of the next node.

By default, no route-policy is defined.



Among the nodes defined in a route-policy, at least one node should be in permit mode. When a route-policy is applied to filtering routing information, if a piece of routing information does not match any node, the routing information will be denied by the route-policy. If all the nodes in the route-policy are in deny mode, all routing information will be denied by the route-policy.

Defining if-match Clauses for a Route-Policy Node

An **if-match** clause defines a matching rule, that is, a filtering condition that the routing information should satisfy for passing the current route-policy node. The matching objects are some attributes of routing information.

Table 309 Define if-match clauses

Operation	Command	Description
Enter system view	**system-view**	-
Enter route-policy view	**route-policy** *route-policy-name* { **permit** | **deny** } **node** *node-number*	-
Define a rule to match the AS path field of BGP routing information	**if-match as-path** *as-number-list*	Optional
Define a rule to match the community attribute of BGP routing information	**if-match community** { *basic-community -number* [**whole-match**] | *adv-community-number* }	Optional
Define a rule to match the destination IP address of routing information	**if-match** { **acl** *acl-number* | **ip-prefix** *ip-prefix-name* }	Optional
Define a rule to match the next-hop interface of routing information	**if-match interface** *interface-type interface-number*	Optional
Define a rule to match the next-hop address of routing information	**if-match ip next-hop** { **acl** *acl-number* | **ip-prefix** *ip-prefix-name* }	Optional
Define a rule to match the routing cost of routing information	**if-match cost** *value*	Optional
Define a rule to match the tag field of RIP or OSPF routing information	**if-match tag** *value*	Optional

By default, no **if-match** clause is defined.



- *The relationship among the **if-match** clauses in a route-policy node is logical "AND". That is, a piece of route information can pass the filter of a node and the actions in **apply** clauses will be taken on it only when all the matching conditions specified by the **if-match** clauses in the node are satisfied.*
- *If no **if-match** clause is defined for a node, all routing information will pass the filter of the node.*

Defining apply Clauses for a Route-Policy Node

apply clauses in a node specify the actions performed after all the filtering conditions of the **if-match clauses** in the node are satisfied. The actions include modifying the attributes of routing information.

Table 310 Define apply clauses

Operation	Command	Description
Enter system view	**system-view**	-
Enter route-policy view	**route-policy** *route-policy-name* { **permit** | **deny** } **node** *node-number*	-
Define an action to add AS numbers before AS path of BGP routing information	**apply as-path** *as-number-1* [*as-number-2* [*as-number-3* ...]]	Optional

Table 310 Define apply clauses

Operation	Command	Description
Define an action to set the community attribute of BGP routing information	**apply community** { **none** | [*aa:nn*] &<1-13> [**no-export-subconfed** | **no-export** | **no-advertise**]* [**additive**] }	Optional
Define a action to set the next-hop address of routing information	**apply ip next-hop** *ip-address*	Optional
Define an action to import routing information into the IS-IS area(s) at specified level(s)	**apply isis** [**level-1** | **level-2** | **level-1-2**]	Optional
Define an action to set the local preference of routing information	**apply local-preference** *local-preference*	Optional
Define an action to set the cost of routing information	**apply cost** *value*	Optional
Define an action to set the cost type of routing information	**apply cost-type** [**internal** | **external**]	Optional
Define an action to set the routing source of routing information	**apply origin** { **igp** | **egp** *as-number* | **incomplete** }	Optional
Define an action to set the tag field of RIP or OSPF routing information	**apply tag** *value*	Optional

By default, no **apply** clause is defined.

Note that, if the **apply cost-type internal** clause is defined for a route-policy node, when all the matching conditions of the node are met, IGP cost will be used as the BGP MED value when the system advertises IGP routes to EBGP peers. The **apply cost** clause takes precedence over the **apply cost-type internal** clause, while the latter takes precedence over the **default med** command.

Defining an IP Prefix List

An ip-prefix (IP prefix list) is identified by its ip-prefix name. Each ip-prefix can include multiple items, and each item, identified by an index-number, can independently specify the match range in network prefix form. Index-numbers specify the matching order of the items in the ip-prefix.

Table 311 Define an IP prefix list

Operation	Command	Description
Enter system view	**system-view**	-
Define an IP prefix list	**ip ip-prefix** *ip-prefix-name* [**index** *index-number*] { **permit** | **deny** } *network len* [**greater-equal** *greater-equal* | **less-equal** *less-equal*]*	Optional

During a matching test, the router checks the items in the ascending order of their index-numbers. Once an item is met, the ip-prefix filtering is passed and no other item will be checked.



Among the items defined in an IP prefix list, at least one item should be in permit mode. The items in deny mode can be used to quickly filter out undesired routing information. But if all the items are in deny mode, no route will pass the filter of the IP prefix list. You can define an item ***permit*** *0.0.0.0 0* ***greater-equal*** *0* ***less-equal*** *32 after the deny-mode items to permit all other routes to pass through.*

AS Path List Configuration

A BGP routing information packet contains an AS path field. AS path list can be used to match the AS path field in BGP routing information to filter out the routing information that does not match.

Table 312 AS path list configuration

Operation	Command	Description
Enter system view	**system-view**	-
Configure AS path list	**ip as-path-acl** *acl-number* { **permit** | **deny** } *as-regular-expression*	Optional

By default, no AS path list is defined.

Community List Configuration

In BGP, community attributes are optional transitive. Some community attributes are globally recognized and they are called standard community attributes. Some are for special purposes and they can be customized.

A route can have one or more community attributes. The speaker of multiple community attributes of a route can act based on one, multiple or all attributes. A router can decide whether to change community attributes before forwarding a route to other peer entity.

Community list is used to identify community information. It falls in to two types: basic community list and advanced community list. The former one's value ranges from 1 to 99, and the latter one's ranges from 100 to 199.

Table 313 Community list configuration

Operation	Command	Description
Enter system view	**system-view**	-
Configure basic community list	**ip community-list** *basic-comm-list-number* { **permit** | **deny** } [*aa:nn*] &<1-12> [**internet** | **no-export-subconfed** | **no-advertise** | **no-export**]*	Optional
Configure advanced community list	**ip community-list** *adv-comm-list-number* { **permit** | **deny** } *comm-regular-expression*	Optional

By default, no BGP community list is defined.

Applying Routing Policy to Route Import

For a routing protocol, you can import the routes discovered by other routing protocols to it to enrich its route knowledge. When doing this, you can adopt a route-policy to filter routing information, so as to import only needed routes. For an import operation, if the destination routing protocol cannot directly use the

routing costs of the source routing protocol, you should specify a routing cost for the imported routes.

*The **import-route** command (used to import routes) is somewhat different in form in different routing protocol views. Refer to the **import-route** command description under the required routing protocol in the command manual.*

Applying Routing Policy to Route Receipt/Advertisement

*The **filter-policy** command (used to apply routing policy to route receipt/advertisement) is somewhat different in form in different routing protocol views. Refer to the **filter-policy** command description under the required routing protocol in the command manual.*

Displaying IP Routing Policy

After the above configuration, execute the **display** command in any view to display and verify the routing policy configuration.

Table 314 Display a route policy

Operation	Command	Description
Display route-policy information	**display route-policy** [*route-policy-name*]	You can execute the **display** command in any view.
Display BGP routes that match an AS path ACL	**display ip as-path-acl** [*acl-number*]	
Display address prefix list information	**display ip ip-prefix** [*ip-prefix-name*]	
Display community list information	**display ip community-list** [*basic-comm-list-number* | *adv-comm-list-number*]	

IP Routing Policy Configuration Example

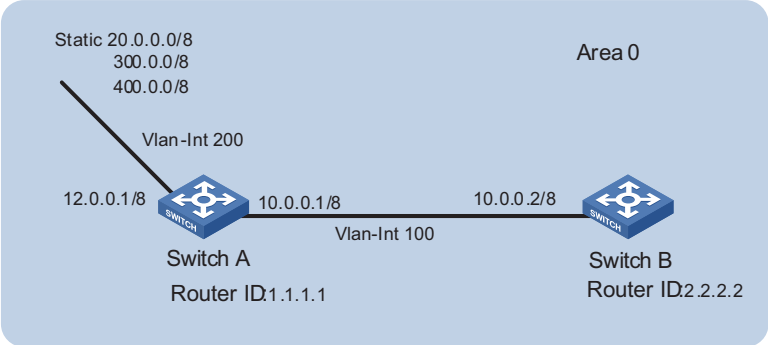
Configuring IP Routing Policy

Network requirements

- As shown in Figure 87, Switch A communicates with Switch B using OSPF protocol. Switch A's router ID is 1.1.1.1 and Switch B's is 2.2.2.2.
- Configure OSPF routing process on Switch A, and configure three static routes.
- Configure a routing policy for Switch A to filter imported static routes. In this example, the routes in 20.0.0.0 and 40.0.0.0 network segments can be imported, but those in 30.0.0.0 network segment will be filtered out.

Network diagram

Figure 87 Filter routing information received



Configuration procedure

1 Configure SwitchA:

Configure the IP addresses of the interfaces.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 100
[SwitchA-Vlan-interface100] ip address 10.0.0.1 255.0.0.0
[SwitchA] interface vlan-interface 200
[SwitchA-Vlan-interface200] ip address 12.0.0.1 255.0.0.0
[SwitchA-Vlan-interface200] quit
```

Configure three static routes.

```
[SwitchA] ip route-static 20.0.0.1 255.0.0.0 12.0.0.2
[SwitchA] ip route-static 30.0.0.1 255.0.0.0 12.0.0.2
[SwitchA] ip route-static 40.0.0.1 255.0.0.0 12.0.0.2
```

Enable the OSPF protocol and specify the ID of the area to which the interface 10.0.0.1 belongs.

```
<SwitchA> system-view
[SwitchA] router id 1.1.1.1
[SwitchA] ospf
[SwitchA-ospf-1] area 0
[SwitchA-ospf-1-area-0.0.0.0] network 10.0.0.0 0.255.255.255
[SwitchA-ospf-1-area-0.0.0.0] quit
[Switch-ospf-1]quit
```

Configure an ACL.

```
[SwitchA] acl number 2000
[SwitchA-acl-basic-2000] rule deny source 30.0.0.0 0.255.255.255
[SwitchA-acl-basic-2000] rule permit source any
[SwitchA-acl-basic-2000] quit
```

Configure a route-policy.

```
[SwitchA] route-policy ospf permit node 10
[SwitchA -route-policy] if-match acl 2000
[SwitchA -route-policy] quit
```

Apply route policy when the static routes are imported.

```
[SwitchA] ospf
[SwitchA-ospf-1] import-route static route-policy ospf
```

2 Configure SwitchB:

Configure the IP address of the interface.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 100
[SwitchB-Vlan-interface100] ip address 10.0.0.2 255.0.0.0
[SwitchB-Vlan-interface100] quit
```

Enable the OSPF protocol and specify the ID of the area to which the interface belongs.

```
[SwitchB] router id 2.2.2.2
[SwitchB] ospf
[SwitchB-ospf-1] area 0
[SwitchB-ospf-1-area-0.0.0.0] network 10.0.0.0 0.255.255.255
[SwitchB-ospf-1-area-0.0.0.0] quit
[SwitchB-ospf-1] quit
```

Display the OSPF routing tables on Switch B and check if the routing policy takes effect.

```
< SwitchB >display ospf 1 routing

  OSPF Process 1 with Router ID 2.2.2.2
                           Routing Tables

Routing for Network
Destination             Cost Type NextHop         AdvRouter        Area
10.0.0.0/8                10 Net  10.0.0.1        1.1.1.1          0.0.0.0

Routing for ASEs
Destination        Cost     Type     Tag  NextHop         AdvRouter
20.0.0.0/8         1        2          1  10.0.0.1        1.1.1.1
40.0.0.0/8         1        2          1  10.0.0.1        1.1.1.1

Total Nets: 1
  Intra Area: 1  Inter Area: 0  ASE: 2  NSSA: 0
```

Troubleshooting IP Routing Policy

Symptom: Routing information cannot be filtered when the routing protocol runs normally.

Solution: Check to see the following requirements are satisfied.

At least one node in a route-policy should be in **permit** mode. When a route-policy is used to filter routing information, if a piece of routing information filters through no node in the route-policy, it means that the route information does not pass the filtering of the route-policy. Therefore, when all the nodes in the route-policy are in the **deny** mode, no routing information will pass the filtering of the route-policy.

At least one item in an ip-prefix list should be in **permit** mode. The items in **deny** mode can be defined first to rapidly filter out the routing information not meeting

the condition. However, if all the items are in the **deny** mode, no route will pass the ip-prefix filtering. You can define the item "**permit** 0.0.0.0 0 less-equal 32" after multiple items in the **deny** mode for all other routes to pass the filtering (if less-equal 32 is not specified, only the default route will be matched).

38 ROUTE CAPACITY CONFIGURATION

Route Capacity Configuration Overview

Introduction

In actual networking applications, there are a large number of routes, especially OSPF routes and BGP routes, in the routing table. If the routing table occupies too much memory, the switch performance will decline.

To solve this problem, the Switch 7750 provide a mechanism to control the size of the routing table; that is, monitoring the free memory in the system to determine whether to add new routes to the routing table and whether to keep the connection of a routing protocol.



CAUTION: *The default system configuration meets the requirements. To avoid decreasing system stability and availability due to improper configuration, it is not recommended to modify the configuration.*

Route Capacity Limitation on the Swtich 7750

Huge routing tables are usually caused by OSPF and BGP routes. Therefore, the route capacity limitation implemented by a Switch 7750 applies to OSPF and BGP routes only but not to static and RIP routes.

When the free memory of the switch is equal to or lower than the lower limit, OSPF or BGP connection will be disconnected and OSPF or BGP routes will be removed from the routing table.

If automatic protocol connection recovery is enabled, when the free memory of the switch restores to a value larger than the safety value, the switch automatically re-establishes the OSPF or BGP connection. If the automatic protocol connection recovery function is disabled, the switch will not reestablish the disconnected OSPF or BGP connection even when the free memory restores to a value larger than the safety value.

Route Capacity Configuration

Route capacity configuration includes:

- Setting the lower limit and the safety value of switch memory,
- Enabling/disabling the switch to recover the disconnected routing protocol automatically.

Setting the Lower Limit and the Safety Value of the Switch Memory

Perform the following configuration in system view.

Table 315 Set the lower limit and the safety value of switch memory

Operation	Command	Description
Enter system view	**system-view**	-
Set the lower limit and the safety value of switch memory	**memory** { **safety** *safety-value* | **limit** *limit-value* }*	Optional *safety-value* defaults to 40 and *limit-value* defaults to 30.



The safety-value must be greater than the limit-value.

Enabling/Disabling Automatic Protocol Connection Recovery

Table 316 Enable automatic protocol recovery

Operation	Command	Description
Enter system view	**system-view**	-
Enable automatic protocol recovery	**memory auto-establish enable**	Optional By default, automatic protocol connection recovery is enabled.
Disable automatic protocol connection recovery	**memory auto-establish disable**	Optional Perform this configuration with caution.



CAUTION: *If automatic protocol recovery is disabled, the broken OSPF or BGP connection will not recover even when the free memory exceeds the safety value. Therefore, do not disable this function if not necessary.*

Displaying Route Capacity Configuration

After the above configuration, you can use the **display** command in any view to display and verify the route capacity configuration.

Table 317 Display route capacity configuration

Operation	Command	Description
Display memory occupancy of a switch	**display memory** [**unit** *unit-id*]	Optional
Display the route capacity related memory setting and state information	**display memory limit**	Optional

39 802.1X CONFIGURATION

Introduction to 802.1x

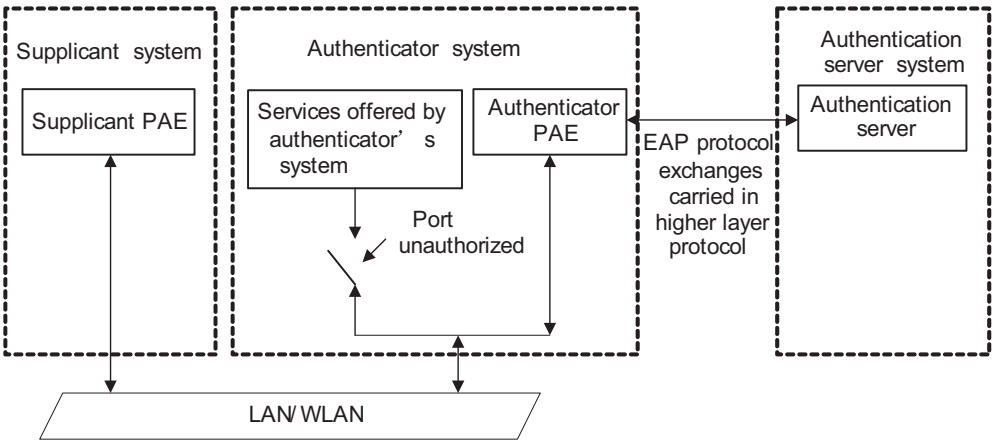
The 802.1x protocol (802.1x for short) was developed by IEEE802 LAN/WAN committee to address security issues of wireless LANs. It was then used in Ethernet as a common access control mechanism for LAN ports to address mainly authentication and security problems.

802.1x is a port-based network access control protocol. It authenticates and controls devices requesting for access in terms of the ports of LAN access control devices. With the 802.1x protocol employed, a user-side device can access the LAN only when it passes the authentication. Those failing to pass the authentication are denied when accessing the LAN, as if they are disconnected from the LAN.

Architecture of 802.1x Authentication

802.1x adopts a client/server architecture with three entities: a supplicant system, an authenticator system, and an authentication server system, as shown in Figure 88.

Figure 88 Architecture of 802.1x authentication



- The supplicant system is an entity residing at one end of the LAN segment and is authenticated by the authenticator system connected to the other end of the LAN segment. The supplicant system is usually a user terminal device. An 802.1x authentication is initiated when a user launches client program on the supplicant system. Note that the client program must support the EAPoL (extensible authentication protocol over LANs).
- The authenticator system authenticates the supplicant system. The authenticator system is usually an 802.1x-supported network device (such as a 3Com series switch). It provides the port (physical or logical) for the supplicant system to access the LAN.
- The authentication server system is an entity that provides authentication service to the authenticator system. Normally in the form of a RADIUS server,

the authentication server system serves to perform AAA (authentication, authorization, and accounting). It also stores user information, such as user name, password, the VLAN a user belongs to, priority, and the ACLs (access control list) applied.

Following are the four basic concept related with the above three entities, namely the PAE, controlled port and uncontrolled port, the valid direction of a controlled port and the way a port is controlled.

PAE

A PAE (port access entity) is responsible for the implementation of algorithm and protocol-related operations in the authentication mechanism.

The authenticator system PAE authenticates the supplicant systems when they log into the LAN and controls the authorizing state (on/off) of the controlled ports according to the authentication result.

The supplicant system PAE responds to the authentication requests received from the authenticator system and submits user authentication information to the authenticator system. It can also send authentication and disconnection requests to the authenticator system PAE.

Controlled port and uncontrolled port

The Authenticator system provides ports for supplicant systems to access a LAN. A port of this kind is divided into a controlled port and an uncontrolled port.

- The uncontrolled port can always send and receive packets. It mainly serves to forward EAPoL packets to ensure that a supplicant system can send and receive authentication requests.
- The controlled port can be used to pass service packets when it is in authorized state. It is blocked when not in authorized state. In this case, no packets can pass through it.
- Controlled port and uncontrolled port are two properties of a access port. Packets reaching an access port are visible to both the controlled port and uncontrolled port of the access port.

The valid direction of a controlled port

When a controlled port is in unauthorized state, you can configure it to be a unidirectional port, which sends packets to supplicant systems only.

By default, a controlled port is a unidirectional port.

The way a port is controlled

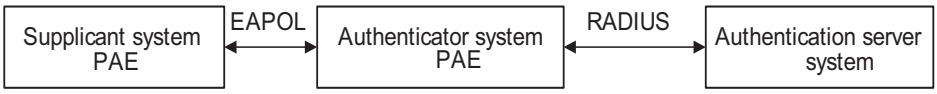
A port of a 3Com series switch can be controlled in the following two ways.

- Port-based authentication. When a port is controlled in this way, all the supplicant systems connected to the port can access the network without being authenticated after one supplicant system among them passes the authentication. And when the authenticated supplicant system goes offline, the others are denied as well.
- MAC address-based authentication. All supplicant systems connected to a port have to be authenticated individually in order to access the network. And when a supplicant system goes offline, the others are not affected.

The Mechanism of an 802.1x Authentication System

IEEE 802.1x authentication system uses extensible authentication protocol (EAP) to exchange information between the supplicant system and the authentication server.

Figure 89 The mechanism of an 802.1x authentication system



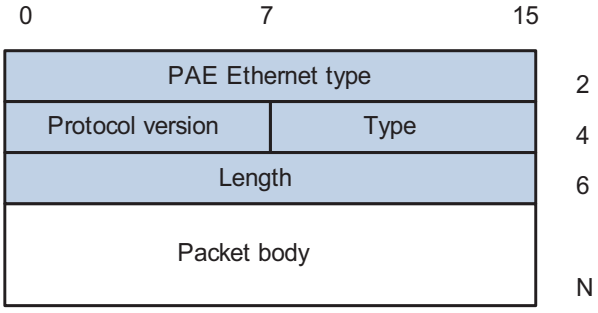
- EAP protocol packets transmitted between the supplicant system and the authenticator system are encapsulated as EAPoL packets.
- EAP protocol packets transmitted between the supplicant system PAE and the RADIUS server can either be encapsulated as EAPoR (EAP over RADIUS) packets or be terminated at system PAEs (The system PAEs then communicate with RADIUS servers through PAP (password authentication protocol) or CHAP (challenge-handshake authentication protocol) protocol packets.)
- When a supplicant system passes the authentication, the authentication server passes the information about the supplicant system to the authenticator system. The authenticator system in turn determines the state (authorized or unauthorized) of the controlled port according to the instructions (accept or reject) received from the RADIUS server.

Encapsulation of EAPoL Messages

The format of an EAPoL packet

EAPoL is a packet encapsulation format defined in 802.1x. To enable EAP protocol packets to be transmitted between supplicant systems and authenticator systems through LANs, EAP protocol packets are encapsulated in EAPoL format. The following figure illustrates the structure of an EAPoL packet.

Figure 90 The format of an EAPoL packet



In an EAPoL packet:

- The PAE Ethernet type field holds the protocol identifier. The identifier for 802.1x is 0x888E.
- The Protocol version field holds the version of the protocol supported by the sender of the EAPoL packet.
- The Type field can be one of the following:

  00: Indicates that the packet is an EAP-packet, which carries authentication information.

  01: Indicates that the packet is an EAPoL-start packet, which initiates authentication.

02: Indicates that the packet is an EAPoL-logoff packet, which sends logging off requests.

03: Indicates that the packet is an EAPoL-key packet, which carries key information packets.

04: Indicates that the packet is an EAPoL-encapsulated-ASF-Alert packet, which is used to support the alerting messages of ASF (alerting standards forum).

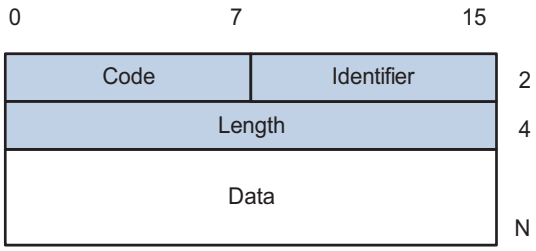
- The Length field indicates the size of the Packet body field. A value of 0 indicates that the Packet Body field does not exist.
- The Packet body field differs with the Type field.

Note that EAPoL-Start, EAPoL-Logoff, and EAPoL-Key packets are only transmitted between the supplicant system and the authenticator system. EAP-packets are encapsulated by RADIUS protocol to allow them successfully reach the authentication servers. Network management-related information (such as alarming information) is encapsulated in EAPoL-Encapsulated-ASF-Alert packets, which are terminated by authenticator systems.

The format of an EAP packet

For an EAPoL packet with the Type value being EAP-packet, the corresponding Packet body is an EAP packet. Its format is illustrated in Figure 91.

Figure 91 The format of an EAP packet



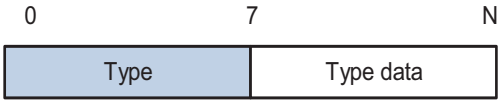
In an EAP packet:

- The Code field specifies the EAP packet type, which can be Request, Response, Success, or Failure.
- The Identifier field is used to match a Response packets with the corresponding Request packet.
- The Length field indicates the size of an EAP packet, which includes the Code, Identifier, Length, and Data fields.
- The Data field differs with the Code field.

A Success or Failure packet does not contain the Data field, so has the Length field of 4.

Figure 92 shows the Data field of Request and Response type packet.

Figure 92 Data fields



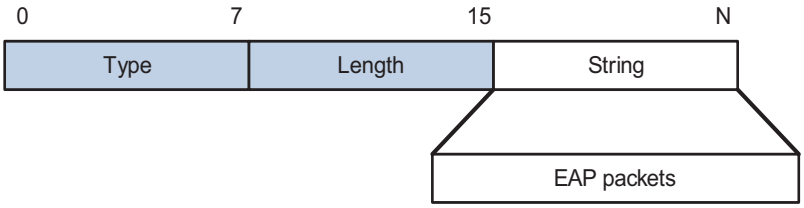
- The Type field specifies the EAP authentication type. A Type value of 1 indicates Identity and that the packet is used to query the identity of the peer. A type value of 4 represents MD5-Challenge (similar to PPP CHAP) and indicates that the packet includes query information.
- The Type Date field differs according to different types of Request and Response packets.

Newly added fields for EAP authentication

Two fields, EAP-message and Message-authenticator, are added to a RADIUS protocol packet for EAP authentication. (Refer to "Introduction to RADIUS" on page 508 for format of a RADIUS protocol packet.)

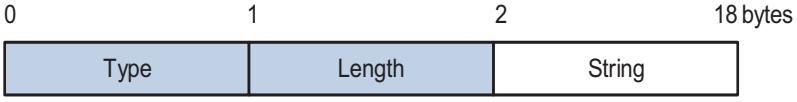
The EAP-message field, shown in Figure 93, is used to encapsulate EAP packets. The maximum size of the string field is 253 bytes. EAP packets with their size larger than 253 bytes are fragmented and stored in multiple EAP-message fields. The type code of the EAP-message field is 79.

Figure 93 The format of an EAP-message field



The Message-authenticator field, as shown in Figure 94, can be used to prevent interception of access request packets during authentications using CHAP, EAP, and so on. A packet with the EAP-message field must also have the Message-authenticator field, otherwise the packet is regarded as invalid and is discarded.

Figure 94 The format of an Message-authenticator field



802.1x Authentication Procedure

A 3Com 6500 series switch can authenticate supplicant systems in EAP terminating mode or EAP relay mode.

EAP relay mode

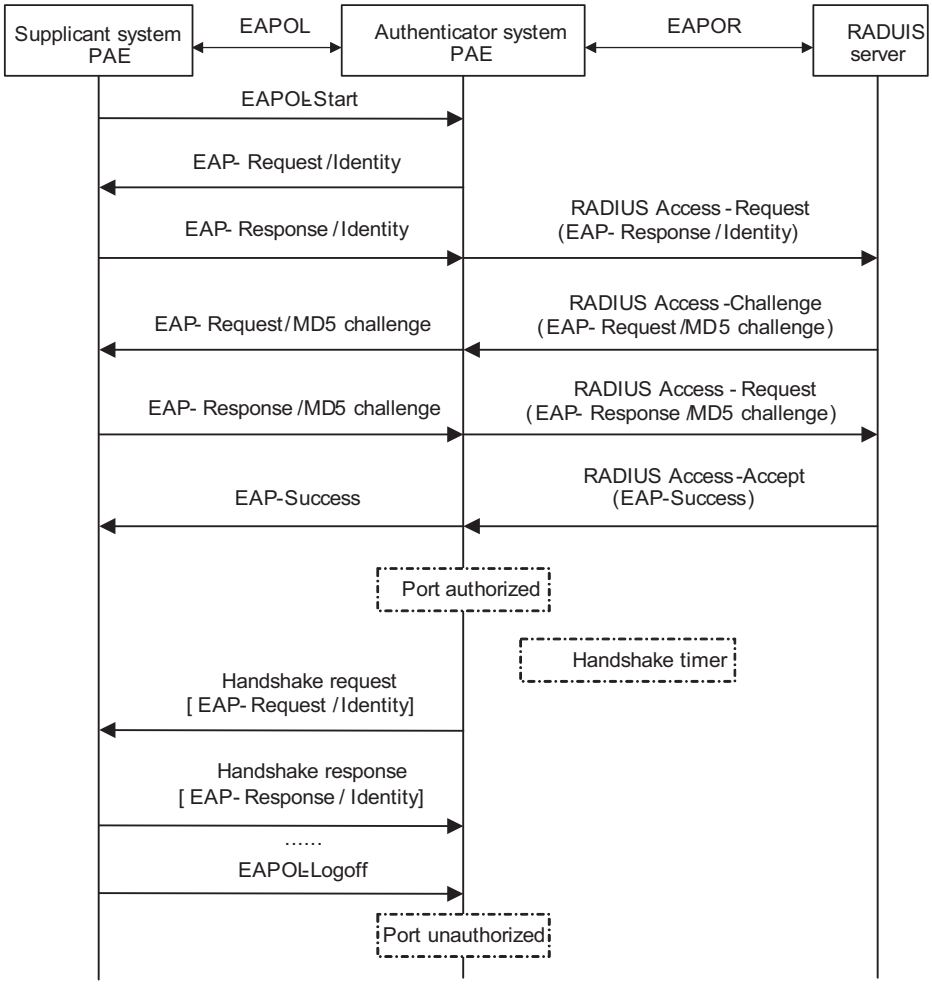
This mode is defined in 802.1x. In this mode, EAP-packets are encapsulated in higher level protocol (such as EAPoR) packets to allow them successfully reach the authentication server. This mode normally requires the RADIUS server to support the two newly-added fields: the EAP-message field (with a value of 79) and the Message-authenticator field (with a value of 80).

Three authentication ways, EAP-MD5, EAP-TLS (transport layer security), and PEAP (protected extensible authentication protocol), are available for the EAP relay mode.

- EAP-MD5 authenticates the supplicant system. The RADIUS server sends MD5 keys (contained in EAP-request/MD5 challenge packets) to the supplicant system, which in turn encrypts the passwords using the MD5 keys.
- EAP-TLS authenticates both the supplicant system and the RADIUS server by checking their security licenses to prevent data from being stolen.
- PEAP creates and uses TLS security channels to ensure data integrity and then performs new EAP negotiations to verify supplicant systems.

Figure 95 describes the basic EAP-MD5 authentication procedure.

Figure 95 802.1x authentication procedure (in EAP relay mode)



The detailed procedure is as follows.

- A supplicant system launches an 802.1x client to initiate an access request through the sending of an EAPoL-start packet to the switch, with its user name and password provided. The 802.1x client program then forwards the packet to the switch to start the authentication process.

- Upon receiving the authentication request packet, the switch sends an EAP-request/identity packet to ask the 802.1x client for the user name.
- The 802.1x program responds by sending an EAP-response/identity packet to the switch with the user name included. The switch then encapsulates the packet in a RADIUS Access-Request packet and forwards it to the RADIUS server.
- Upon receiving the user name from the switch, the RADIUS server retrieves the user name, finds the corresponding password by matching the user name in its database, encrypts the password using a randomly-generated key, and sends the key to the switch through an RADIUS access-challenge packet. The switch then sends the key to the 802.1x client.
- Upon receiving the key(encapsulated in an EAP-request/MD5 challenge packet) from the switch, the client program encrypts the password of the supplicant system with the key and sends the encrypted password (contained in an EAP-response/MD5 challenge packet) to the RADIUS server through the switch. (The encryption is irreversible.)
- The RADIUS server compares the received encrypted password (contained in a RADIUS access-request packet) with the locally-encrypted password. If the two match, it will then send feedbacks (through a RADIUS access-accept packet and an EAP-success packet) to the switch to indicate that the supplicant system is authorized.
- The switch changes the state of the corresponding port to accepted state to allow the supplicant system access the network.
- The supplicant system can also terminate the authenticated state by sending EAPoL-Logoff packets to the switch. The switch then changes the port state from accepted to rejected.



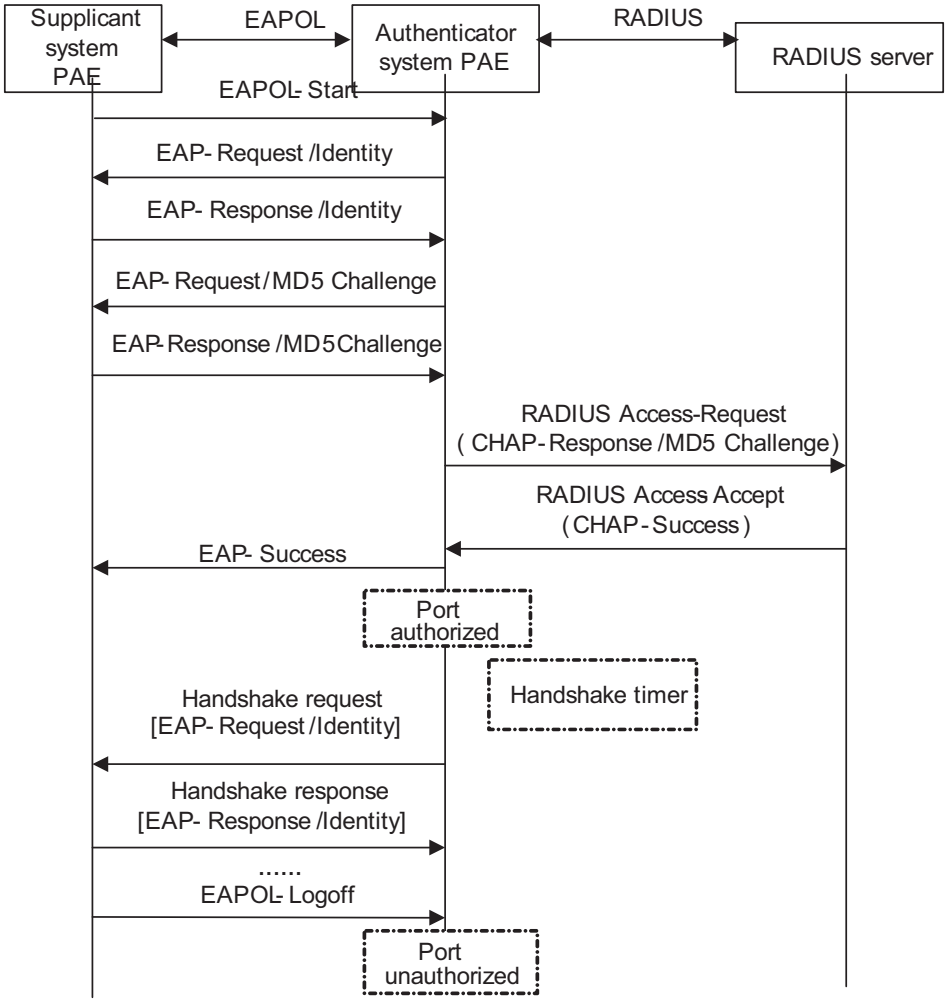
In EAP relay mode, packets are not modified during transmission. Therefore if one of the three ways are used (that is, PEAP, EAP-TLS, or EAP-MD5) to authenticate, ensure that the authenticating ways used on the supplicant system and the RADIUS server are the same. However for the switch, you can simply enable the EAP relay mode by using the ***dot1x authentication-method eap*** *command.*

EAP terminating mode

In this mode, packet transmission is terminated at authenticator systems and the EAP packets are converted to RADIUS packets. Authentication and accounting are accomplished through RADIUS protocol.

In this mode, PAP or CHAP is employed between the switch and the RADIUS server. The authentication procedure (assuming that CHAP is employed between the switch and the RADIUS server) is illustrated in Figure 96.

Figure 96 802.1x authentication procedure (in EAP terminating mode)



The authentication procedure in EAP terminating mode is the same as that in the EAP relay mode except that the randomly-generated key in the EAP terminating mode is generated by the switch, and that it is the switch that sends the user name, the randomly-generated key, and the supplicant system-encrypted password to the RADIUS server for further authentication.

802.1x Timer

In 802.1 x authentication, the following timers are used to ensure that the supplicant system, the switch, and the RADIUS server interact in an orderly way:

- Transmission timer (**tx-period**): This timer sets the tx-period and is triggered by the switch in one of the following two cases: The first case is when the client requests for authentication. The switch sends a unicast request/identity packet to a supplicant system and then enables the transmission timer. The switch sends another request/identity packet to the supplicant system if the supplicant system fails to send a reply packet to the switch when this timer times out. The second case is when the switch authenticates the 802.1x client who does not request for authentication actively. The switch sends multicast request/identity packets continuously through the port enabled with 802.1x function, with the interval of tx-period.

- Supplicant system timer (**supp-timeout**): This timer sets the supp-timeout period and is triggered by the switch after the switch sends a request/challenge packet to a supplicant system. The switch sends another request/challenge packet to the supplicant system if the supplicant system fails to respond when this timer times out.
- RADIUS server timer (**server-timeout**): This timer sets the server-timeout period. The switch sends another authentication request packet if the RADIUS server fails to respond when this timer times out.
- Handshake timer (**handshake-period**): This timer sets the handshake-period and is triggered after a supplicant system passes the authentication. It sets the interval for a switch to send handshake request packets to online users. If you set the number of retries to N by using the **dot1x retry** command, an online user is considered offline when the switch does not receive response packets from it in a period N times of the handshake-period.
- Re-authentication timer (**reauth-period**): Within this timer period, a supplicant system initializes 802.1x re-authentication.
- Quiet-period timer (**quiet-period**): This timer sets the quiet-period. When a supplicant system fails to pass the authentication, the switch quiets for the set period (set by the quiet-period timer) before it processing another 802.1x-relatedauthentication request initiated by the supplicant system.
- **ver-period**: This timer sets the client version request timer. If the supplicant system does not send the version response packets within the set period, the switch sends another version request packet.

802.1x Implementation on the Switch 7750

In addition to the earlier mentioned 802.1x features, a Switch 7750 is also capable of the following:

- Cooperating with a CAMS server to perform proxy detection, such as detecting login through proxy and multiple network adapters
- Checking client version
- Implementing the Guest VLAN function

Proxy detection

A Switch 7750 implements 802.1x proxy detection to check:

- Supplicant systems logging on through proxies
- Supplicant systems logging on through IE proxies
- Whether or not a supplicant system logs in through more than one network modules (that is, whether or not more than one network adapters are active in a supplicant system when the supplicant system logs in).

In response to any of the three cases, a switch can optionally take the following measures:

- Disconnect the supplicant system and send Trap packets (achieved via the **dot1x supp-proxy-check logoff** command.)
- Send Trap packets without disconnecting the supplicant system (achieved via the **dot1x supp-proxy-check trap** command.)

This function needs the support of 802.1x clients and CAMS:

- The 802.1x clients are capable of detecting multi-network adapter, proxies, and IE proxies.
- CAMS is configured to disable the use of multiple network adapters, proxies, or IE proxies.

By default, an 802.1x client program allows use of multiple network adapters, a proxy server, and an IE proxy server. If CAMS is configured to disable use of multiple network adapters, proxies, or IE proxies, it prompts the 802.1x client to disable use of multiple network adapters, proxies, or IE proxies through messages after the supplicant system passes the authentication.



- *The client-checking function needs the support of 3Com's 802.1x client program.*
- *The proxy detecting function should be enabled on both the 802.1x client program and CAMS. The client version detecting should be enabled on the switch (achieved via the* ***dot1x version-check*** *command).*

Client version detection

With the 802.1x client-version-checking function enabled, a switch will check the version and validity of an 802.1x client to prevent unauthorized users or users with earlier versions of 802.1x from logging in.

This function makes the switch to send version-requesting packets again if the 802.1x client fails to send version-reply packet to the switch before the version-checking timer times out.



The client-version-checking function needs the support of 3Com's 802.1x client program.

The Guest VLAN function

The Guest VLAN function enables supplicant systems that do not pass the authentication to access a LAN in a restrained way.

With the Guest VLAN function enabled, supplicant systems that do not have 802.1x client installed can access specific network resources. They can also upgrade their 802.1x clients without being authenticated.

With this function enabled:

- The switch multicasts trigger packets to all 802.1x-enabled ports.
- After the maximum number retries have been made and there are still ports that have not sent any response back, the switch will then add these ports into the Guest VLAN.
- Users belonging to the Guest VLAN can access the resources of the Guest VLAN without being authenticated. But they need to be authenticated before accessing external resources.

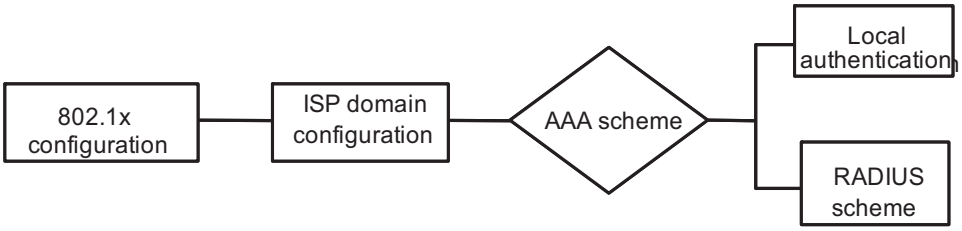
Normally, the Guest VLAN function is coupled with the dynamic VLAN delivery function.

Refer to *"Configuring Dynamic VLAN Assignment" on page 522* for detailed information about dynamic VLAN assignment function.

802.1x Configuration

802.1x provides a solution for authenticating users. To implement this solution, you need to execute 802.1x-related commands. You also need to configure AAA schemes on switches and to specify the authentication scheme (RADIUS authentication scheme or local authentication scheme).

Figure 97 802.1x configuration



- 802.1x users use domain names to associate with the ISP domains configured on switches
- Configure the AAA scheme (a local authentication scheme or the RADIUS scheme) to be adopted in the ISP domain.
- If you specify to use the RADIUS scheme, that is to say the supplicant systems are authenticated by a remote RADIUS server, you need to configure the related user names and passwords on the RADIUS server and perform RADIUS client-related configuration on the switches.
- If you specify to adopt a local authentication scheme, you need to configure user names and passwords manually on the switches. Users can pass the authentication through 802.1x client if they provide the user names and passwords that match with those stored in the switches.
- You can also specify to adopt RADIUS authentication scheme, with a local authentication scheme as a backup. In this case, the local authentication scheme is adopted when the RADIUS server fails.

Refer to "AAA Configuration" on page 518 for detailed information about AAA configuration.

Basic 802.1x Configuration

To utilize 802.1x features, you need to perform basic 802.1x configuration.

Prerequisites

- Configure ISP domain and its AAA scheme, specify the authentication scheme (RADIUS or a local scheme).
- Ensure that the service type is configured as **lan-access** (by using the **service-type** command) for local authentication scheme.

Configuring Basic 802.1x Functions

Table 318 Configure basic 802.1x functions

Operation	Command	Description
Enter system view	**system-view**	-
Enable 802.1x globally	**dot1x**	Required By default, 802.1x is disabled globally.

Table 318 Configure basic 802.1x functions

Operation	Command	Description
Enable 802.1x for specified ports	Use the following command in system view: **dot1x** [**interface** *interface-list*] Use the following command in port view: **dot1x**	Required By default, 802.1x is disabled for all ports.
Set port access control mode for specified ports	**dot1x port-control** { **authorized-force** | **unauthorized-force** | **auto** } [**interface** *interface-list*]	Optional By default, an 802.1x-enabled port operates in an **auto** mode.
Set port access method for specified ports	**dot1x port-method** { **macbased** | **portbased** } [**interface** *interface-list*]	Optional The default port access method is MAC-address-based (that is, the **macbased** keyword is used by default).
Set authentication method for 802.1x users	**dot1x authentication-method** { **chap** | **pap** | **eap** }	Optional By default, a switch performs CHAP authentication in EAP terminating mode.
Enable 802.1x re-authentication	In system view: **dot1x re-authenticate** [**interface** *interface-list*] In port view: **dot1x re-authenticate**	Optional By default, 802.1x re-authentication is disabled on all ports.

CAUTION:

- *802.1x-related configurations can all be performed in system view. Port access control mode and port access method can also be configured in port view.*
- *If you perform a configuration in system view and do not specify the interface-list argument, the configuration applies to all ports. Configurations performed in Ethernet port view apply to the current Ethernet port only and the interface-list argument is not needed in this case.*
- *802.1x configurations take effect only after you enable 802.1x both globally and for specified ports.*
- *Changing the access control method on a port by the **dot1x port-method** command will forcibly log out the online 802.1x users on the port.*
- *You can set 802.1x re-authentication timer on the switch either by using the **dot1x reauth-period** command or through the RADIUS server. Upon receiving an Access-Accept packet, with Termination-Action attribute value set to 1, from the server, the switch performs authentication at an interval of the session-timeout value of the Access-Accept packet. In actual authentication, the switch uses the latest time value obtained as the authentication interval.*
- *After re-authentication is enabled on a port, you cannot change the dynamic VLAN delivery attribute value for the port; if you do so, the re-authentication will cause users to be offline.*

802.1x-Related Parameter Configuration

Table 319 Configure 802.1x timers and the maximum number of users

Operation	Command	Description
Enter system view	**system-view**	-
Configure the maximum number of concurrent on-line users for specified ports	In system view: **dot1x max-user** *user-number* [**interface** *interface-list*] In port view: **dot1x max-user** *user-number*	Optional By default, up to 1,024 concurrent on-line users are allowed on each port.
Configure the maximum retry times to send request packets	**dot1x retry** *max-retry-value*	Optional By default, the maximum retry times to send a request packet is 2. That is, the authenticator system sends a request packet to a supplicant system for up to two times by default.
Configure 802.1x timers	**dot1x timer** { **handshake-period** *handshake-period-value* | **reauth-period** *reauth-period-value* | **quiet-period** *quiet-period-value* | **tx-period** *tx-period-value* | **supp-timeout** *supp-timeout-value* | **server-timeout** *server-timeout-value* | **ver-period** *ver-period-value* }	Optional The default values of 802.1x timers are as follows: ■ *handshake-period-value:* 15 seconds ■ *reauth-period-value:* 3,600 seconds ■ *quiet-period-value:* 60 seconds ■ *tx-period-value:* 30 seconds ■ *supp-timeout-value:* 30 seconds ■ *server-timeout-value:* 100 seconds ■ *ver-period-value:* 30 seconds
Trigger the quiet-period timer	**dot1x quiet-period**	Optional By default, a quiet-period timer is disabled.



- *As for the **dot1x max-user** command, if you execute it in system view without specifying the interface-list argument, the command applies to all ports. You can also use this command in port view. In this case, this command applies to the current port only and the interface-list argument is not needed.*
- *As for the configuration of 802.1x timers, the default values are recommended.*

Advanced 802.1x Configuration

Advanced 802.1x configurations, as listed below, are all optional.

- CAMS cooperation configuration, including multiple network adapters detecting, proxy detecting, and so on.
- Client version checking configuration
- DHCP -triggered authentication
- Guest VLAN configuration

Prerequisites Configuration of basic 802.1x

Configuring Proxy Checking

This function needs the support of 802.1x client program and CAMS, as listed below.

- The 802.1x clients must be able to check whether multiple network modules, proxy servers, or IE proxy servers are used on the user devices.
- On CAMS, enable the function that forbids clients from using multiple network modules, a proxy server, or an IE proxy.

By default, the use of multiple network modules, proxy server, and IE proxy are allowed on 802.1x client. If you specify CAMS to disable use of multiple network modules, proxy server, and IE proxy, CAMS sends messages to 802.1x client to request the latter to disable the use of multiple network modules, proxy server, and IE proxy when a user passes the authentication.

Table 320 Configure user proxy checking

Operation	Command	Description
Enter system view	**system-view**	-
Enable global proxy checking function	**dot1x supp-proxy-check** { **logoff** | **trap** }	Required By default, the global 802.1X proxy checking is disabled.
Enable proxy checking for a port	In system view: **dot1x supp-proxy-check** { **logoff** | **trap** } [**interface** *interface-list*]	Required By default, the 802.1X proxy checking is disabled for the port.
	In port view: **dot1x supp-proxy-check** { **logoff** | **trap** }	



- *The proxy checking function needs the support of 3Com's 802.1x client program.*
- *The configuration listed in Table 320 takes effect only when it is performed on CAMS as well as on the switch and the client version checking function is enabled on the switch (by the **dot1x version-check** command).*

Configuring Client Version Checking

Table 321 Configure client version checking

Operation	Command	Description
Enter system view	**system-view**	-
Enable 802.1x client version checking	**dot1x version-check** [**interface** *interface-list*]	Required By default, 802.1x client version checking is disabled on a port.
Configure the maximum number of retires to send version checking request packets	**dot1x retry-version-max** *max-retry-version-value*	Optional Defaults to 3.

Table 321 Configure client version checking

Operation	Command	Description
Configure the client-version-checking period timer	**dot1x timer ver-period** *ver-period-value*	Optional The default *ver-period-value* is 30 seconds

*As for the **dot1x version-user** command, if you execute it in system view without specifying the interface-list argument, the command applies to all ports. You can also use this command in port view. In this case, this command applies to the current port only and the interface-list argument is not needed.*

Enabling DHCP-triggered Authentication

After performing the following configuration, 802.1X allows running DHCP on access users, and triggers authentication when the user dynamically applies IP address.

Table 322 Enable DHCP-triggered authentication

Operation	Command	Description
Enter system view	**system-view**	-
Enable DHCP-triggered authentication	**dot1x dhcp-launch**	Optional By default, DHCP-triggered authentication is disabled.

Configuring Guest VLAN

Table 323 Configure Guest VLAN

Operation	Command	Description
Enter system view	**system-view**	-
Configure port access method	**dot1x port-method** { **macbased** | **portbased** }	Optional The default port access method is MAC-address-based. That is, the **macbased** keyword is used by default.
Enable the Guest VLAN function	**dot1x guest-vlan** *vlan-id* [**interface** *interface-list*]	Required By default, the Guest VLAN function is disabled.

CAUTION:

- *The Guest VLAN function is available only when the switch operates in a port-based authentication mode.*
- *Only one Guest VLAN can be configured for each switch.*

Displaying and Debugging 802.1x

After performing the above configurations, you can display and verify the 802.1x-related configuration by executing the **display** command in any view.

You can clear 802.1x-related statistics information by executing the **reset** command in user view.

Table 324 Display and debug 802.1x

Operation	Command	Description
Display the configuration, session, and statistics information about 802.1x	**display dot1x** [**sessions** | **statistics**] [**interface** *interface-list*]	You can execute the display command in any view
Clear 802.1x-related statistics information	**reset dot1x statistics** [**interface** *interface-list*]	You can execute the reset command in user view

Configuration Example

802.1x Configuration Example

Network requirements

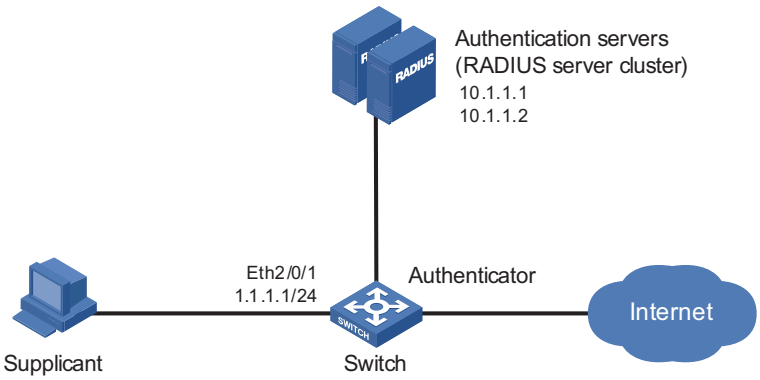
- Authenticate users on all ports to control their accesses to the Internet. The switch operates in MAC address-based access control mode. The access control mode is MAC-address-based.
- All supplicant systems that pass the authentication belong to the default domain named "aabbcc.net". The domain can accommodate up to 30 users. As for authentication, a supplicant system is authenticated locally if the RADIUS server fails. And as for accounting, a supplicant system is disconnected by force if the RADIUS server fails. The name of an authenticated supplicant system is not suffixed with the domain name. A connection is terminated if the total size of the data passes through it during a period of 20 minutes is less than 2,000 bytes. All connected clients belong to the same default domain: aabbcc.net, which accommodates up to 30 clients. Authentication is performed either on the RADIUS server, or locally (in case that the RADIUS server fails to respond). A client is disconnected in one of the following two situations: RADIUS accounting fails; the connected user has not included the domain name in the username, and there is a continuous below 2000 bytes of traffic for over 20 minutes.
- The switch is connected to a server comprising of two RADIUS servers whose IP addresses are 10.1.1.1 and 10.1.1.2. The RADIUS server with an IP address of 10.1.1.1 operates as the primary authentication server and the secondary accounting server. The other operates as the secondary authentication server and primary accounting server. The password for the switch and the authentication RADIUS servers to exchange message is "name". And the password for the switch and the accounting RADIUS servers to exchange message is "money". The switch sends another packet to the RADIUS servers again if it sends a packet to the RADIUS server and does not receive response for 5 seconds with a maximum number of retries of 5. And the switch sends a real-time accounting packet to the RADIUS servers once in every 15 minutes. A user name is sent to the RADIUS servers with the domain name truncated. Connected to the switch is a server group comprised of two RADIUS servers whose IP addresses are 10.1.1.1 and 10.1.1.2 respectively, with the former being the primary authentication and the secondary counting server, and the latter the secondary authentication and the primary counting server. Configure the interaction password between the switch and the authenticating RADIUS server to be "name", and "money" for interaction between the switch and the counting RADIUS. Configure the waiting period for the switch to resend packets to the RADIUS server to be 5 seconds, that is, if after 5 seconds the RADIUS still has not sent any responses back, the switch will resend packets.

Configure the number of times that a switch resends packets to the RADIUS server to be 5. Configure the switch to send real-time counting packets to the RADIUS server every 15 minutes with the domain names removed from the user name beforehand.

- The user name and password for local 802.1x authentication are "localuser" and "localpass" (in plain text) respectively. The idle disconnecting function is enabled.

Network diagram

Figure 98 Network diagram for AAA configuration with 802.1x and RADIUS enabled



Configuration procedure

Following configuration covers the major AAA/RADIUS configuration commands. You can refer to "AAA Configuration" on page 518 and "RADIUS Configuration" on page 525 for information about these commands. Configuration on the client and the RADIUS servers is omitted.

Enable 802.1x globally.

```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] dot1x
```

Enable 802.1x for Ethernet2/0/1 port.

```
[SW7750] dot1x interface Ethernet 2/0/1
```

Set the access control method to be MAC-address-based (can be omitted as MAC-address-based is the default configuration).

```
[SW7750] dot1x port-method macbased interface Ethernet 2/0/1
```

Create a RADIUS scheme named "radius1" and enter RADIUS scheme view.

```
[SW7750] radius scheme radius1
```

Assign IP addresses to the primary authentication and accounting RADIUS servers.

```
[SW7750-radius-radius1] primary authentication 10.1.1.1
[SW7750-radius-radius1] primary accounting 10.1.1.2
```

Assign IP addresses to the secondary authentication and accounting RADIUS server.

```
[SW7750-radius-radius1] secondary authentication 10.1.1.2
[SW7750-radius-radius1] secondary accounting 10.1.1.1
```

Set the password for the switch and the authentication RADIUS servers to exchange messages.

```
[SW7750 -radius-radius1] key authentication name
```

Set the password for the switch and the accounting RADIUS servers to exchange messages.

```
[SW7750-radius-radius1] key accounting money
```

Set the interval and the number of retries for the switch to send packets to the RADIUS servers. # Set the timer and the number of times that a switch will resend packets to the RADIUS server

```
[SW7750-radius-radius1] timer 5
[SW7750-radius-radius1] retry 5
```

Set the timer for the switch to send real-time accounting packets to the RADIUS servers.

```
[SW7750-radius-radius1] timer realtime-accounting 15
```

Configure to send the user name to the RADIUS server with the domain name removed beforehand.

```
[SW7750-radius-radius1] user-name-format without-domain
[SW7750-radius-radius1] quit
```

Create the domain named "aabbcc.net" and enter its view.

```
[SW7750] domain enable aabbcc.net
```

Specify to adopt radius1 as the RADIUS scheme of the user domain. If RADIUS server is invalid, specify to adopt local authentication scheme.

```
[SW7750-isp-aabbcc.net] scheme radius-scheme radius1 local
```

Specify the maximum number of users the user domain can accommodate to 30.

```
[SW7750-isp-aabbcc.net] access-limit enable 30
```

Enable the idle disconnecting function and set the related parameters.

```
[SW7750-isp-aabbcc.net] idle-cut enable 20 2000
[SW7750-isp-aabbcc.net] quit
```

Configure the default user domain named "aabbcc.net".

```
[SW7750] domain default enable aabbcc.net
```

Create a local access user account.

```
[SW7750] local-user localuser
[SW7750-luser-localuser] service-type lan-access
[SW7750-luser-localuser] password simple localpass
```

40 HABP CONFIGURATION

Introduction to HABP

With 802.1x enabled, a switch authenticates and then authorizes 802.1x-enabled ports. Packets can be forwarded only by authorized ports. If ports connected to the switch are not authenticated and authorized by 802.1x, their received packets will be filtered. This means that users can no longer manage the attached switches. To address this problem, 3Com authentication bypass protocol (HABP) has been developed.

An HABP packet carries the MAC addresses of the attached switches with it. It can bypass the 802.1x authentications when traveling between HABP-enabled switches, through which management devices can obtain the MAC addresses of the attached switches and thus the management of the attached switches is feasible.

An HABP packet encapsulates the MAC address of the connected switch to a given port. This allows HABP packets to bypass 802.1x authentication and to be forwarded between HABP-enabled switches. Therefore, the management devices can get the MAC addresses of their attached switches to manage them effectively.

HABP is implemented by HABP server and HABP client. Normally, an HABP server sends HABP request packets regularly to HABP clients to collect the MAC addresses of the attached switches. HABP clients respond to the HABP request packets and forward the HABP request packets to lower-level switches. HABP servers usually reside on management devices and HABP clients usually on attached switches.

For ease of switch management, it is recommended that you enable HABP for 802.1x-enabled switches.

HABP Server Configuration

With the HABP server launched, a management device sends HABP request packets regularly to the attached switches to collect their MAC addresses. You need also to configure the interval on the management device for an HABP server to send HABP request packets.

Table 325 Configure an HABP server

Operation	Command	Description
Enter system view	**system-view**	-
Enable HABP	**habp enable**	Required HABP is enabled by default.

Table 325 Configure an HABP server

Operation	Command	Description
Configure the current switch to be an HABP server	**habp server vlan** *vlan-id*	Required By default, a switch operates as an HABP client after you enable HABP on the switch, and if you want to use the switch as a management switch, you must configure the switch to be an HABP server.
Configure the interval to send HABP request packets.	**habp timer** *interval*	Optional The default interval for an HABP server to send HABP request packets is 20 seconds.

HABP Client Configuration

HABP clients reside on switches attached to HABP servers. After you enable HABP for a switch, the switch operates as an HABP client by default. So you only need to enable HABP on a switch to make it an HABP client.

Table 326 Configure an HABP client

Operation	Command	Description
Enter system view	**system-view**	-
Enable HABP	**habp enable**	Optional HABP is enabled by default. And a switch operates as an HABP client after you enable HABP for it.

Displaying HABP

After performing the above configuration, you can display and verify your HABP-related configuration by execute the **display** command in any view.

Table 327 Display HABP

Operation	Command	Description
Display HABP configuration and status information	**display habp**	You can execute the **display** command in any view
Display the MAC address table maintained by HABP	**display habp table**	
Display statistics on HABP traffic	**display habp traffic**	

HABP Configuration Example

Network requirements

As shown in Figure 99, Switch B operates as a 3Com authentication bypass protocol (HABP) server, Switch A operates as a HABP client. Both Switch A and Switch B are in VLAN 2.

- Switch A and Switch B are interconnected through trunk ports GigabitEthernet2/0/1 (Switch A) and GigabitEthernet2/0/2 (Switch B).
- VLAN 2 is the default of the two ports.
- The two ports permit packets of all the VLANs.

Network diagram

Figure 99 Network diagram for HABP configuration



Configuration procedure

1 Configure Switch B.

Enable HABP globally.

```
<SW7750>system-view
[SW7750]habp enable
```

Configure the HABP server.

```
[SW7750]habp server vlan 2
```

Enable the 802.1x globally.

```
[SW7750]dot1x
 802.1x is enabled globally.
```

Enable the 802.1x on GigabitEthernet2/0/2.

```
[SW7750]interface GigabitEthernet 2/0/2
[SW7750-GigabitEthernet2/0/2]dot1x
 802.1x is enabled on port GigabitEthernet2/0/2.
```

2 Configure Switch A

Enable HABP globally.

```
<SW7750>system-view
System View: return to User View with Ctrl+Z.
[SW7750]habp enable
```

Verify the configuration on the server.

```
[SW7750]display habp table
MAC             Holdtime  Receive Port
000f-e200-5004      41        GigabitEthernet2/0/2
000f-e200-5002     41        GigabitEthernet2/0/2
```

41 MULTICAST OVERVIEW

"Router" or a router icon in this document refers to a router in a generic sense or an Ethernet switch running a routing protocol. This will not be otherwise described in this manual.

Multicast Overview

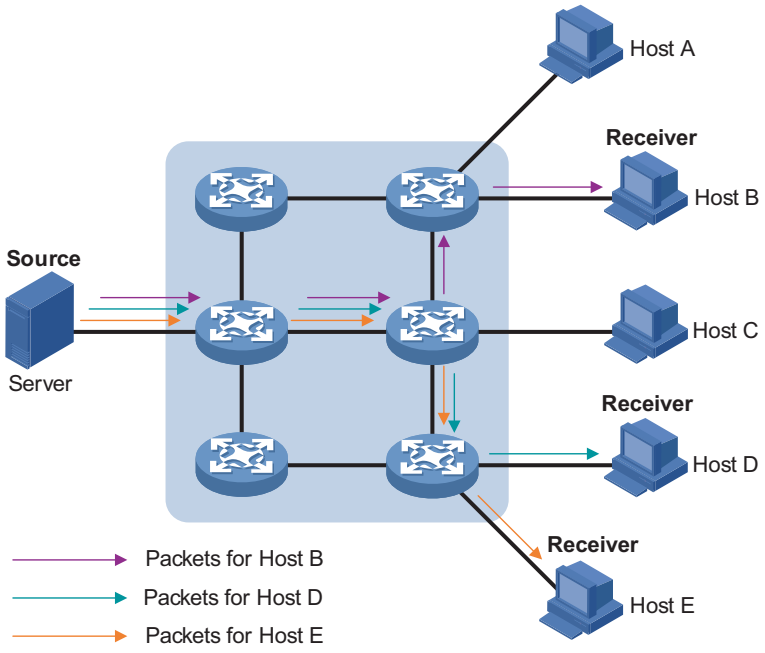
With development of networks on the Internet, more and more interaction services such as data, voice, and video services are running on the networks. In addition, services highly dependent on bandwidth and real-time data interaction, such as e-commerce, web conference, online auction, video on demand (VoD), and tele-education have come into being. These services have higher requirements for information security, legal use of paid services, and network bandwidth.

In the network, packets are sent in three modes: unicast, broadcast and multicast. The following sections describe and compare data interaction processes in unicast, broadcast, and multicast.

Information Transmission in the Unicast Mode

In unicast, the system establishes a separate data transmission channel for each user requiring this information, and sends separate copy information to the user, as shown in Figure 100:

Figure 100 Information transmission in the unicast mode



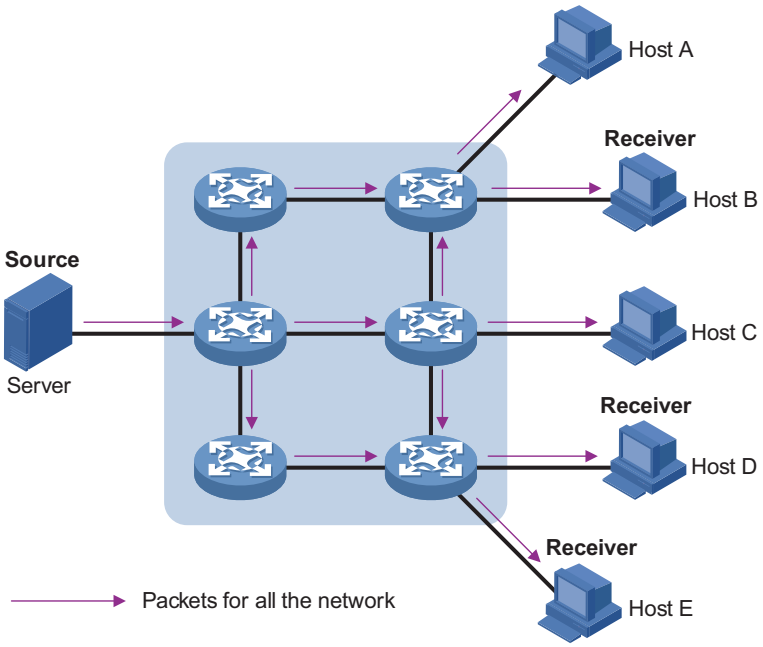
Assume that users B, D and E need this information. The source server establishes transmission channels for the devices of these users respectively. As the

transmitted traffic over the network is proportional to the number of users that receive this information, when a large number of users need this information, the server must send many pieces of information with the same content to the users. Therefore, the limited bandwidth becomes the bottleneck in information transmission. This shows that unicast is not good for the transmission of a great deal of information.

Information Transmission in the Broadcast Mode

When you adopt broadcast, the system transmits information to all users on a network. Any user on the network can receive the information, no matter the information is needed or not. Figure 101 shows information transmission in broadcast mode.

Figure 101 Information transmission in the broadcast mode



Assume that users B, D, and E need the information. The source server broadcasts this information through routers, and users A and C on the network also receive this information. The security and payment of the information cannot be guaranteed.

As we can see from the information transmission process, the security and legal use of paid service cannot be guaranteed. In addition, when only a small number of users on the same network need the information, the utilization ratio of the network resources is very low and the bandwidth resources are greatly wasted.

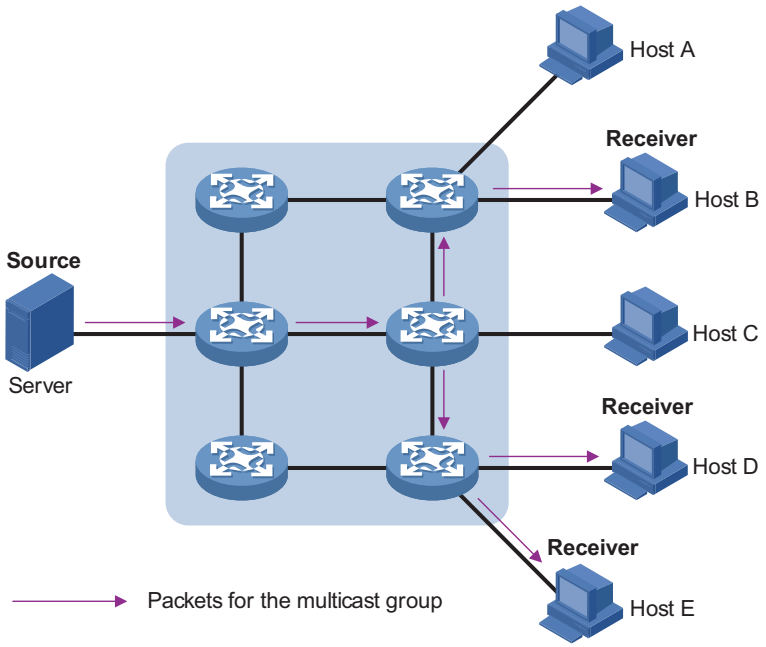
Therefore, broadcast is disadvantageous in transmitting data to specified users; moreover, broadcast occupies large bandwidth.

Information Transmission in the Multicast Mode

As described in the previous sections, unicast is suitable for networks with sparsely distributed users, whereas broadcast is suitable for networks with densely distributed users. When the number of users requiring information is not certain, unicast and broadcast deliver a low efficiency.

Multicast solves this problem. When some users on a network require specified information, the multicast information sender (namely, the multicast source) sends the information only once. With tree-type routes established for multicast data packets through a multicast routing protocol, the packets are duplicated and distributed at the nearest nodes as shown in Figure 102:

Figure 102 Information transmission in the multicast mode



Assume that users B, D and E need the information. To transmit the information to the right users, it is necessary to group users B, D and E into a receiver set. The routers on the network duplicate and distribute the information based on the distribution of the receivers in this set. Finally, the information is correctly delivered to users B, D, and E.

The advantages of multicast over unicast are as follows:

- No matter how many receivers exist, there is only one copy of the same multicast data flow on each link.
- With the multicast mode used to transmit information, an increase of the number of users does not add to the network burden remarkably.

The advantages of multicast over broadcast are as follows:

- A multicast data flow can be sent only to the receiver that requires the data.
- Multicast brings no waste of network resources and makes proper use of bandwidth.

In the multicast mode, network components can be divided in to the following roles:

- An information sender is referred to as a multicast source.
- Multiple receivers receiving the same information form a multicast group. Multicast group is not limited by physical area.

- Each receiver receiving multicast information is a multicast group member.
- A router providing multicast routing is a multicast router. The multicast router can be a member of one or multiple multicast groups, and it can also manage members of the multicast groups.



CAUTION: *A multicast source does not necessarily belong to a multicast group. A multicast source sends packets to a multicast group, and it is not necessarily a receiver. Multiple multicast sources can send packets to the same multicast group at the same time.*

There may be routers that do not support multicast on the network. A multicast router encapsulates multicast packets in unicast IP packets in the tunnel mode, and then sends them to the neighboring multicast routers through the router that do no support multicast. The neighboring multicast routers remove the header of the unicast IP packets, and then continue to multicast the packets, thus avoiding changing the network structure greatly.

Advantages and Applications of Multicast

Advantages of multicast

Advantages of multicast include:

- Enhanced efficiency: Multicast decreases network traffic and reduces server load and CPU load.
- Optimal performance: Multicast reduces redundant traffic.
- Distributive application: Multicast makes multiple-point application possible.

Application of multicast

The multicast technology effectively addresses the issue of point-to-multipoint data transmission. By enabling high-efficiency point-to-multipoint data transmission, over an IP network, multicast greatly saves network bandwidth and reduces network load.

Multicast provides the following applications:

- Applications of multimedia and flow media, such as Web TV, Web radio, and real-time video/audio conferencing.
- Communication for training and cooperative operations, such as remote education.
- Database and financial applications (stock), and so on.
- Any point-to-multiple-point data application.

Multicast Architecture

The purpose of IP multicast is to transmit information from a multicast source to receivers in the multicast mode and to satisfy information requirements of receivers. You should be concerned about:

- Host registration: What receivers reside on the network?
- Technologies of discovering a multicast source: Which multicast source should the receivers receive information from?
- Multicast addressing mechanism: Where should the multicast source transports information to?

- Multicast routing: How is information transported?

IP multicast is a kind of peer-to-peer service. Based on the protocol layer sequence from bottom to top, the multicast mechanism contains addressing mechanism, host registration, multicast routing, and multicast application:

- Addressing mechanism: Information is sent from a multicast source to a group of receivers through multicast addresses.
- Host registration: A receiving host joins and leaves a multicast group dynamically to implement membership registration.
- Multicast routing: A router or switch establishes a packet distribution tree and transports packets from a multicast source to receivers.
- Multicast application: A multicast source must support multicast applications, such as video conferencing. The TCP/IP protocol stack must support the function of sending and receiving multicast information.

Multicast Address

As receivers are multiple hosts in a multicast group, you should be concerned about the following questions:

- What destination should the information source send the information to in the multicast mode?
- How to select the destination address, that is, how does the information source know who the user is?

These questions are about multicast addressing. To enable the communication between the information source and members of a multicast group (a group of information receivers), network-layer multicast addresses, namely, IP multicast addresses must be provided. In addition, a technology must be available to map IP multicast addresses to link-layer MAC multicast addresses. The following sections describe these two types of multicast addresses:

IP multicast address

Internet Assigned Numbers Authority (IANA) categorizes IP addresses into five classes: A, B, C, D, and E. Unicast packets use IP addresses of Class A, B, and C based on network scales. Class D IP addresses are used as destination addresses of multicast packets. Class D address must not appear in the IP address field of a source IP address of IP packets. Class E IP addresses are reserved for future use.

In unicast data transport, a data packet is transported hop by hop from the source address to the destination address. In an IP multicast environment, there are a group of destination addresses (called group address), rather than one address. All the receivers join a group. Once they join the group, the data sent to this group of addresses starts to be transported to the receivers. All the members in this group can receive the data packets. This group is a multicast group.

A multicast group has the following characteristics:

- The membership of a group is dynamic. A host can join and leave a multicast group at any time.
- A multicast group can be either permanent or temporary.

- A multicast group whose addresses are assigned by IANA is a permanent multicast group. It is also called reserved multicast group.

Note that:

- The IP addresses of a permanent multicast group keep unchanged, while the members of the group can be changed.
- There can be any number of, or even zero, members in a permanent multicast group.
- Those IP multicast addresses not assigned to permanent multicast groups can be used by temporary multicast groups.

Class D IP addresses range from 224.0.0.0 to 239.255.255.255. For details, see Table 328.

Table 328 Range and description of Class D IP addresses

Class D address range	Description
224.0.0.0 to 224.0.0.255	Reserved multicast addresses (IP addresses for permanent multicast groups). The IP address 224.0.0.0 is reserved. Other IP addresses can be used by routing protocols.
224.0.1.0 to 231.255.255.255 233.0.0.0 to 238.255.255.255	Available any-source multicast (ASM) multicast addresses (IP addresses of temporary groups). They are valid for the entire network.
232.0.0.0 to 232.255.255.255	Available source-specific multicast (SSM) multicast group addresses.
239.0.0.0 to 239.255.255.255	Local management multicast addresses, which are used in the local use only.

As specified by IANA, the IP addresses ranging from 224.0.0.0 to 224.0.0.255 are reserved for network protocols on local networks. The following table lists commonly used reserved IP multicast addresses:

Table 329 Reserved IP multicast addresses

Class D address range	Description
224.0.0.1	Address of all hosts
224.0.0.2	Address of all multicast routers
224.0.0.3	Unassigned
224.0.0.4	Distance vector multicast routing protocol (DVMRP) routers
224.0.0.5	Open shortest path first (OSPF) routers
224.0.0.6	Open shortest path first designated routers (OSPF DR)
224.0.0.7	Shared tree routers
224.0.0.8	Shared tree hosts
224.0.0.9	RIP-2 routers
224.0.0.11	Mobile agents
224.0.0.12	DHCP server / relay agent
224.0.0.13	All protocol independent multicast (PIM) routers
224.0.0.14	Resource reservation protocol (RSVP) encapsulation
224.0.0.15	All core-based tree (CBT) routers

Table 329 Reserved IP multicast addresses

Class D address range	Description
224.0.0.16	The specified subnetwork bandwidth management (SBM)
224.0.0.17	All SBMS
224.0.0.18	Virtual router redundancy protocol (VRRP)
224.0.0.19- 224.0.0.255	Other protocols

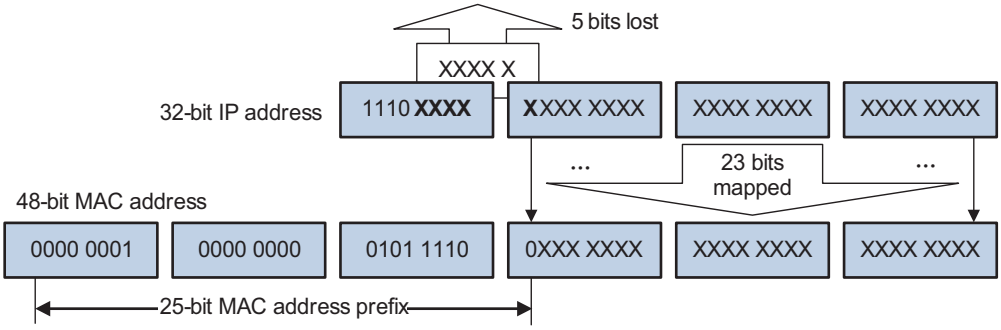
Like having reserved the private network segment 10.0.0.0/8 for unicast, IANA has also reserved the network segments ranging from 239.0.0.0 to 239.255.255.255 for multicast. These are administratively scoped addresses. With the administratively scoped addresses, you can define the range of multicast domains flexibly to isolate IP addresses between different multicast domains, so that the same multicast address can be used in different multicast domains without causing collisions.

Ethernet multicast MAC address

When a unicast IP packet is transported in an Ethernet network, the destination MAC address is the MAC address of the receiver. When a multicast packet is transported in an Ethernet network, a multicast MAC address is used as the destination address because the destination is a group with an uncertain number of members.

As stipulated by IANA, the high-order 24 bits of a multicast MAC address are 0 x 01005e, while the low-order 23 bits of a MAC address are the low-order 23 bits of the multicast IP address. Figure 103 describes the mapping relationship:

Figure 103 Mapping relationship between multicast IP address and multicast MAC address

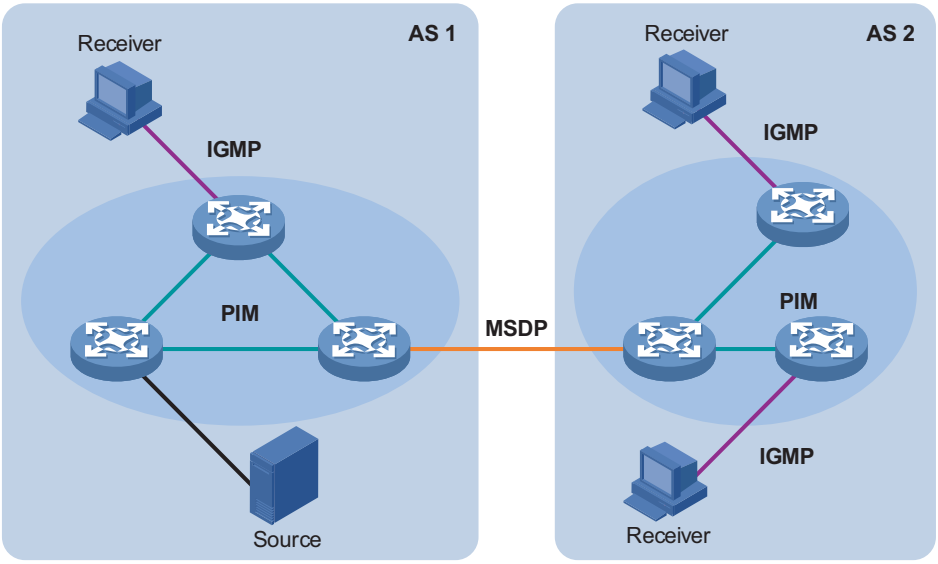


The high-order four bits of the IP multicast address are 1110, representing the multicast ID. Only 23 bits of the remaining 28 bits are mapped to a MAC address Thus five bits of the multicast IP address are lost. As a result, 32 IP multicast addresses are mapped to the same MAC address.

IP Multicast Protocols

IP multicast protocols include the multicast group management protocol and the multicast routing protocol. Figure 104 describes the positions of the protocols related to multicast in the network.

Figure 104 Positions of protocols related to multicast



Multicast group management protocol

Internet group management protocol (IGMP) is adopted between a host and its directly-connected multicast routers. This protocol defines the mechanism of establishing and maintaining multicast group membership between hosts and multicast routers.

There are three versions for IGMP currently, including IGMPv1, IGMPv2 and IGMPv3. A new version is compatible with the old ones.

Multicast routing protocols

A multicast routing protocol operates between multicast routers to establish and maintain multicast routes and forward multicast packets accurately and effectively. A multicast route establishes a loop-free data transport path (also known as multicast distribution tree) from a data source to multiple receivers.

Multicast routes include intra-domain routes and inter-domain routes:

- Intra-domain multicast routes have been quite mature. Protocol independent multicast (PIM) is the most commonly used protocol currently. PIM transmits information to receivers by means of multicast source discovery and multicast distribution tree establishment. According to forwarding mechanisms, PIM includes PIM dense mode (PIM-DM) and PIM sparse mode (PIM-SM).
- The key problem for inter-domain routes is how to transmit information between autonomous systems (AS). Currently, multicast source discovery protocol is a relatively mature solution.

Forwarding Mechanism of Multicast Packets

In a multicast model, a multicast source host transports information to the multicast group, which is identified by the multicast group address in the destination address field of an IP data packet. Unlike a unicast model, a multicast model must forward data packets to multiple external interfaces so that all receiver sites can receive the packets. Therefore the forwarding process of multicast is more complicated than unicast.

In order to guarantee the transmission of multicast packets in the network, multicast packets must be forwarded based on unicast routing tables or those specially provided to multicast (such as an MBGP multicast routing table). In addition, to prevent the interfaces from receiving the same information from different peers, routers must check the receiving interfaces. This check mechanism is reverse path forwarding (RPF) check, which is the basis of performing multicast forwarding for most multicast routing protocols.

Based on source addresses, multicast routers judge whether multicast packets come from specified interfaces, that is, RPF check determines whether inbound interfaces are correct by comparing the interfaces that the packets reach with the interfaces that the packets should reach. If the router resides on a shortest path tree (SPT), the interface that multicast packets should reach points to the multicast source. If the router resides on a rendezvous point tree (RPT), the interface that multicast packets should reach points to the rendezvous point (RP). When multicast data packets reach the router, if RPF check passes, the router forwards the data packets based on multicast forwarding entries; otherwise, the data packets are dropped.

42 GMRP CONFIGURATION

GMRP Overview

GMRP (GARP Multicast Registration Protocol), based on GARP, is used for maintaining multicast registration information of the switch. All GMRP-capable switches can receive multicast registration information from other switches, dynamically update local multicast registration information, and send their own local multicast registration information to other switches. This information switching mechanism keeps consistency of the multicast information maintained by every GMRP-supporting device in the same switching network.

A host sends a GMRP Join message, if it is interested in joining a multicast group. After receiving the message, the switch adds the port on which the message was received to the multicast group, and broadcasts the message throughout the VLAN where the receiving port resides. In this way, the multicast source in the VLAN gets aware of the existence of the multicast group member. When the multicast source sends multicast packets to a group, the switch only forwards the packets to ports connected to the members of that group, thereby implementing Layer 2 multicast in the VLAN.

Configuring GMRP

The main tasks in GMRP configuration include:

- Enable GMRP globally
- Enable GMRP on a port

GMRP must be enabled globally before it is enabled on a port.

Enabling GMRP Globally

Table 330 Enable GMRP globally

Operation	Command	Description
Enter system view	**system-view**	-
Enable GMRP globally.	**gmrp**	Required Disabled by default.

Enabling GMRP on the Port

Perform the following configuration in Ethernet port view.

Table 331 Enable/Disable GMRP on the port

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Enable GMRP on the port	**gmrp**	Required Disabled by default.

Displaying and Maintaining GMRP

After the above-described configuration, execute the **display** command in any view to display the running of the GMRP configuration, and to verify the effect of the configuration.

Table 332 Display and debug GMRP

Operation	Command	Description
Display the GMRP statistics information	**display gmrp statistics** [**interface** *interface-list*]	Available in any view
Display the GMRP global status	**display gmrp status**	

GMRP Configuration Example

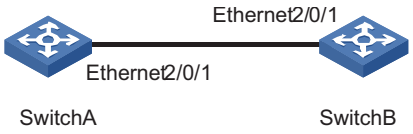
Enabling GMRP

Network requirements

Implement dynamic registration and update of multicast information between switches.

Network diagram

Figure 105 Networking diagram for GMRP configuration



Configuration procedure

Configure SwitchA:

Enable GMRP globally.

```
<SW7750> system-view
[SW7750] gmrp
GMRP is enabled globally.
```

Enable GMRP on the port.

```
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] gmrp
GMRP is enabled on port Ethernet 2/0/1.
```

Configure SwitchB:

Enable GMRP globally.

```
<SW7750> system-view
[SW7750] gmrp
GMRP is enabled globally.
```

Enable GMRP on the port.

```
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] gmrp
GMRP is enabled on port Ethernet 2/0/1.
```

43 IGMP SNOOPING CONFIGURATION

Overview

IGMP Snooping Fundamentals

Internet group management protocol snooping (IGMP Snooping) is a multicast control mechanism running on Layer 2 switch. It is used to manage and control multicast groups.

When the IGMP messages transferred from the hosts to the router pass through the Layer 2 switch, the switch uses IGMP Snooping to analyze and process the IGMP messages, as shown in Table 333.

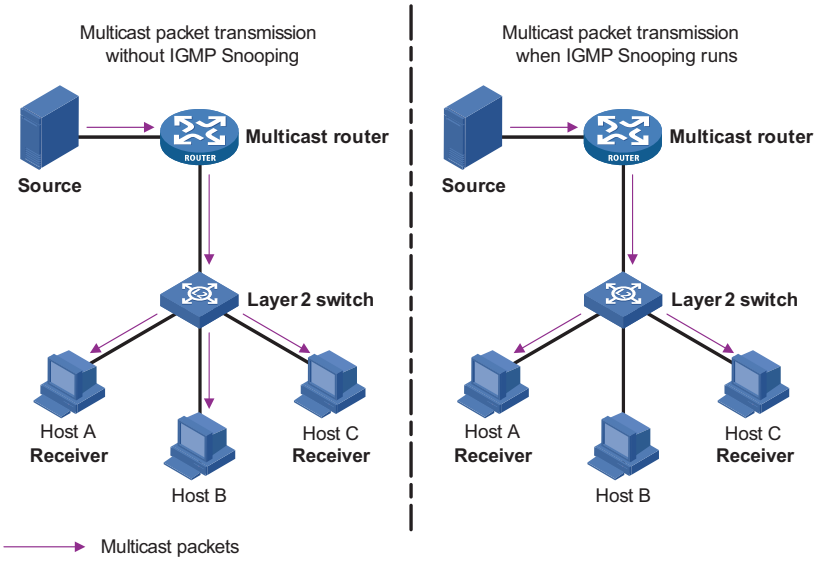
Table 333 IGMP message processing on the switch

Received message type	Sender	Receiver	Switch processing
IGMP host report message	Host	Switch	Add the host to the corresponding multicast group.
IGMP leave message	Host	Switch	Remove the host from the multicast group.

By listening to IGMP messages, the switch establishes and maintains MAC multicast address tables at data link layer, and uses the tables to forward the multicast packets delivered from the router.

As shown in Figure 106, multicast packets are broadcasted at Layer 2 when IGMP Snooping is disabled and multicast at Layer 2 when IGMP Snooping is enabled.

Figure 106 Multicast packet transmission with or without IGMP Snooping being enabled



IGMP Snooping Implementation

IGMP Snooping terminologies

- Router port: the switch port directly connected to the multicast router.
- Multicast member port: a switch port connected to a multicast group member (a host in a multicast group).
- MAC multicast group: a multicast group identified by a MAC multicast address and maintained by the switch.
- Router port aging timer, multicast member port aging timer, and query response timer are described in Table 334.

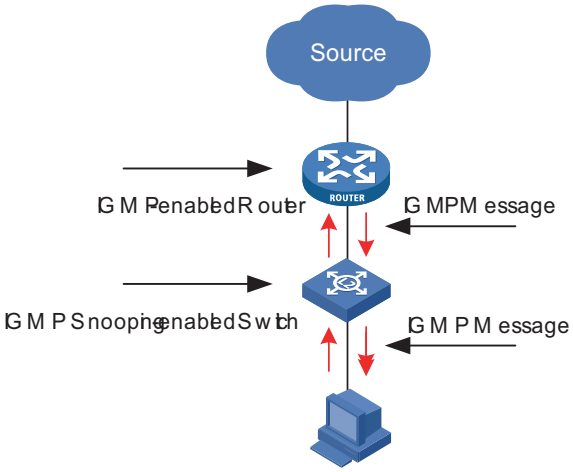
Table 334 IGMP Snooping timers

Timer	Setting	Packet normally received before timeout	Timeout action on the switch
Router port aging timer	Aging time of the router port	IGMP general query message/PIM message/DVMRP probe message	Consider that this port is not a router port any more.
Multicast member port aging timer	Aging time of the multicast member ports	IGMP message	Send an IGMP group-specific query message to the multicast member port.
Query response timer	Query response timeout time	IGMP report message	Remove the port from the member port list of the multicast group.

Layer 2 multicast with IGMP Snooping

The switch runs IGMP Snooping to listen to IGMP messages and map the host, the port corresponding to the host, and the corresponding multicast MAC address.

Figure 107 IGMP Snooping implementation



To implement Layer 2 multicast, the switch processes four different types of IGMP messages it received, as shown in Table 335.

Table 335 IGMP Snooping messages

Message	Sender	Receiver	Purpose	Action of the multicast member switch			
IGMP general query message	Multicast router and multicast switch	Multicast member switch and host	Query if the multicast groups contain any member	Check if the message comes from the original router port	If yes, reset the aging timer of the router port		
					If not, notify the multicast router that a member is in a multicast group and start the aging timer for the router port		
IGMP group-specific query message	Multicast router and multicast switch	Multicast member switch and host	Query if a specific IGMP multicast group contains any member	Send an IGMP group-specific query message to the IP multicast group being queried.			
IGMP host report message	Host	Multicast router and multicast switch	Apply for joining a multicast group, or respond to an IGMP query message	Check if the IP multicast group has a corresponding MAC multicast group	If yes, check if the port exists in the MAC multicast group	If yes, add the IP multicast group address to the MAC multicast group table.	
						If not, add the port to the MAC multicast group, reset the aging timer of the port and check if the corresponding IP multicast group exists.	If yes, add the port to the IP multicast group.
							If not, create an IP multicast group and add the port to it.
					If not: ■ Create a MAC multicast group and notify the multicast router that a member is ready to join the multicast group. ■ Add the port to the MAC multicast group and start the aging timer of the port. ■ Add all router ports in the VLAN owning this port to the MAC multicast group. ■ Create an IP multicast group and add the port to it.		

Table 335 IGMP Snooping messages

Message	Sender	Receiver	Purpose	Action of the multicast member switch	
IGMP leave message	Host	Multicast router and multicast switch	Notify the multicast router and multicast switch that the host is leaving its multicast group.	Multicast router and multicast switch send IGMP specific group query message(s) to the multicast group whose member host sends leave messages to check if the multicast group has any members and enable the corresponding query timer.	If the multicast group responds, the switch checks whether the port is the last host port corresponding to the MAC multicast group. ■ If yes, remove the correspondi ng MAC multicast group and IP multicast group ■ If no, remove only those entries that correspond to this port in the MAC multicast group, and remove the correspondi ng IP multicast group entries
					If no response is received from the multicast group before the timer times out, notify the router to remove this multicast group node from the multicast tree



CAUTION: *An IGMP-Snooping-enabled Switch 7750 Ethernet switch judges whether the multicast group exists when it receives an IGMP leave packet sent by a host in a multicast group. If this multicast group does not exist, the switch will drop the IGMP leave packet instead of forwarding it.*

IGMP Snooping Configuration

Table 336 IGMP Snooping configuration tasks

Operation	Description	Related section
Enable IGMP Snooping	Required	"Enabling IGMP Snooping" on page 431
Configure IGMP Snooping version	Optional	"Configuring the Version of IGMP Snooping" on page 431

Table 336 IGMP Snooping configuration tasks

Operation	Description	Related section
Configure timers	Optional	"Configuring Timers" on page 432
Enable IGMP fast leave	Optional	"Enabling IGMP Fast Leave for a Port or All Ports" on page 432
Configure IGMP Snooping filter	Optional	"Configuring IGMP Snooping Filtering ACLs" on page 433
Configure to limit the number of multicast groups on a port	Optional	"Configuring to Limit Number of Multicast Groups on a Port" on page 434
Configure IGMP Snooping querier	Optional	"Configuring IGMP Snooping Querier" on page 434
Configure suppression on IGMP host report messages	Optional	"Configuring Suppression on IGMP Host Report Messages" on page 435
Configure simulated joining	Optional	"Configuring IGMP Snooping Simulated Joining" on page 436
Configure multicast VLAN	Optional	"Configuring Multicast VLAN" on page 437

Enabling IGMP Snooping

You can use the command here to enable IGMP Snooping so that it can establish and maintain MAC multicast group forwarding tables at layer 2.

Table 337 Enable IGMP Snooping

Operation	Command	Description
Enter system view	**system-view**	-
Enable IGMP Snooping globally	**igmp-snooping enable**	Required IGMP Snooping is disabled globally.
Enter VLAN view	**vlan** *vlan-id*	-
Enable IGMP Snooping on the VLAN	**igmp-snooping enable**	Required By default, IGMP Snooping is disabled on the VLAN.

CAUTION:

- *Although both Layer 2 and Layer 3 multicast protocols can run on the same switch simultaneously, they cannot run simultaneously on a VLAN or its corresponding VLAN interface.*
- *Before configuring IGMP Snooping in VLAN view, you must enable IGMP Snooping globally in system view. Otherwise, the IGMP Snooping feature cannot be enabled in VLAN view.*

Configuring the Version of IGMP Snooping

With the development of multicast technologies, IGMPv3 has found increasingly wide application. In IGMPv3, a host can not only join a specific multicast group but also explicitly specify to receive or reject the information from a specific multicast source. Working with PIM-SSM, IGMPv3 enables hosts to join specific multicast sources and groups directly, greatly simplifying multicast routing protocols and optimizing the network topology.

Table 338 Configure the version of IGMP Snooping

Operation	Command	Description
Enter system view	**system-view**	-
Enter VLAN view	**vlan** *vlan-id*	-
Configure the version of IGMP Snooping	**igmp-snooping version** *version-number*	Optional The default IGMP Snooping version is version 2.

CAUTION:

- *Before configuring the IGMP Snooping version, you must enable IGMP Snooping in the VLAN.*
- *Different multicast group addresses should be configured for different multicast sources because IGMPv3 Snooping cannot distinguish multicast data from different sources to the same multicast group.*

Configuring Timers

This configuration task is to manually configure the aging timer of the router port, the aging timer of the multicast member ports, and the query response timer.

- If the switch receives no general IGMP query message from a router within the aging time of the router port, the switch removes the router port from the port member lists of all MAC multicast groups.
- If the switch receives no IGMP host report message, it sends an IGMP group-specific query message to the port and enable the query response timer of the IP multicast group.
- If the switch receives no IGMP host report message within the aging time of the member port, it sends IGMP group-specific query to the port and enables the query response timer of the IP multicast group.

Table 339 Configure timers

Operation	Command	Description
Enter system view	**system-view**	-
Configure the aging timer of the router port	**igmp-snooping router-aging-time** *seconds*	Optional By default, the aging time of the router port is 105 seconds.
Configure the query response timer	**igmp-snooping max-response-time** *seconds*	Optional By default, the query response timeout time is 10 seconds.
Configure the aging timer of the multicast member port	**igmp-snooping host-aging-time** *seconds*	Optional By default, the aging time of multicast member ports is 260 seconds

Enabling IGMP Fast Leave for a Port or All Ports

Normally, when receiving an IGMP Leave message, the switch does not immediately remove the port from the multicast group, but sends an IGMP group-specific query message. If no response is received in a given period, it then removes the port from the multicast group.

If the IGMP fast leave feature is enabled, when receiving an IGMP Leave message, the switch immediately removes the port from the multicast group. When a port has only one user, enabling the IGMP fast leave feature on the port can save bandwidth.

Enabling the IGMP fast leave feature for all ports globally

Table 340 Enable the IGMP fast leave feature for all ports globally

Operation	Command	Description
Enter system view	**system-view**	-
Enable the fast leave feature from the multicast group of the specific VLAN for all port	**igmp-snooping fast-leave** [**vlan** *vlan-list*]	Optional By default, the fast leave feature from a multicast group for all ports is disabled.

Enabling the fast leave feature for a port

Table 341 Enable the fast leave feature for a port

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Enable the fast leave feature from the multicast group of the specific VLAN for a port	**igmp-snooping fast-leave** [**vlan** *vlan-list*]	Optional By default, the fast leave feature from a multicast group for a port is disabled.

Configuring IGMP Snooping Filtering ACLs

You can configure multicast filtering ACLs on the switch ports connected to user ends so as to use the IGMP Snooping filter function to limit the multicast streams that the users can access. With this function, you can treat different VoD users in different ways by allowing them to access the multicast streams in different multicast groups.

In practice, when a user orders a multicast program, an IGMP report message is generated. When the message arrives at the switch, the switch examines the multicast filtering ACL configured on the access port to determine if the port can join the corresponding multicast group or not. If yes, it adds the port to the forward port list of the multicast group. If not, it drops the IGMP report message and does not forward the corresponding data stream to the port. In this way, you can control the multicast streams that users can access.

Make sure that ACL rules have been configured before configuring this feature.

Configuring IGMP Snooping filtering ACLs globally

Table 342 Configure IGMP Snooping filtering ACLs globally

Operation	Command	Description
Enter system view	**system-view**	-

Table 342 Configure IGMP Snooping filtering ACLs globally

Operation	Command	Description
Enable IGMP Snooping filter in system view	**igmp-snooping group-policy** *acl-number* [**vlan** *vlan-list*]	Required ■ You can configure the ACL to filter the IP addresses of corresponding multicast group. ■ By default, the multicast filtering feature is disabled.

Configuring IGMP Snooping filtering ACLs for a port

Table 343 Configure IGMP Snooping filtering ACLs for a port

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Configure the multicast filtering feature for the port	**igmp-snooping group-policy** *acl-number* [**vlan** *vlan-list*]	Required ■ You can configure the ACL to filter the IP addresses of corresponding multicast group. ■ By default, the multicast filtering feature is disabled.

- *One port can belong to multiple VLANs. Only one ACL rule can be configured on each of the VLANs to which the port belongs.*
- *If the port does not belong to the VLAN where the command is configured, the configured ACL rule does not take effect.*
- *If no ACL rule is configured in the command, the multicast packets of all the multicast groups are rejected.*

Configuring to Limit Number of Multicast Groups on a Port

With a limit imposed on the number of multicast groups on the switch port, users can no longer have as many multicast groups as they want when demanding multicast group programs. Thereby, the bandwidth on the port is controlled.

Table 344 Configure to limit number of multicast groups on a port

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Configure the number of multicast groups on a port	**igmp-snooping group-limit** *limit* [**vlan** *vlan-list* [**overflow-replace**] **| overflow-replace**]	Optional The number of multicast groups on a port is 256

Configuring IGMP Snooping Querier

In an IP multicast network running IGMP, a multicast router is responsible for sending IGMP general queries, so that all Layer 3 multicast devices can establish and maintain multicast forwarding entries, thus to forward multicast traffic correctly at the network layer. This router or Layer 3 switch is called IGMP querier.

However, a Layer 2 multicast switch does not support IGMP, and therefore does have an IGMP querier to send general queries by default. By enabling IGMP Snooping querier on a Layer 2 switch in a VLAN where multicast traffic needs to be Layer-2 switched only and no multicast routers are present, the Layer 2 switch will act as a querier to send IGMP general queries, thus allowing multicast forwarding entries to be established and maintained at the data link layer.

You can also configure the source address and interval of general queries to be sent from the IGMP Snooping querier.

Table 345 Configure IGMP Snooping querier

Operation	Command	Description
Enter system view	**system-view**	-
Enable IGMP Snooping	**igmp-snooping enable**	Required By default, IGMP Snooping is disabled.
Enter VLAN view	**vlan** *vlan-id*	-
Enable IGMP Snooping	**igmp-snooping enable**	Required By default, IGMP Snooping is disabled.
Enable IGMP Snooping querier	**igmp-snooping querier**	Required By default, IGMP Snooping querier is disabled.
Configure the interval between IGMP general queries	**igmp-snooping query-interval** *seconds*	Optional By default, the interval between IGMP general queries is 60 seconds.
Configure the source IP address of IGMP general queries	**igmp-snooping general-query source-ip** { **current-interface** | *ip-address* }	Optional By default, the source IP address of IGMP general queries is 0.0.0.0.

Configuring Suppression on IGMP Host Report Messages

When a Layer 2 switch receives IGMP host report messages from a host in a multicast group, the switch will forward the packets to the port of a Layer 3 switch that is connected to it. In this way, a Layer 3 switch will receive the same IGMP host report messages from multiple hosts in a multicast group when there are multiple hosts in this multicast group.

When suppression on IGMP host report messages is enabled, in a query interval, the Layer 2 switch will forward only the first IGMP host report message from a multicast group to the Layer 3 switch, and drop the other IGMP host report messages from the same multicast group.

Table 346 Configure suppression on IGMP host report messages

Operation	Command	Description
Enter system view	**system-view**	-
Configure suppression on IGMP host report messages	**report-aggregation**	Required By default, suppression on IGMP host report messages is disabled.

Configuring IGMP Snooping Simulated Joining

Generally, hosts running IGMP respond to the IGMP query messages of the IGMP querier. If hosts fail to respond for some reason, the multicast router may consider that there is no member of the multicast group on the local subnet and remove the corresponding path.

To avoid this from happening, you can configure a port of the IGMP-enabled VLAN interface as a multicast group member. When the port receives IGMP query messages, the simulated member host will respond. As a result, the subnet attached to the Layer 3 interface can continue to receive multicast traffic.

Through this configuration, the following functions can be implemented:

- When an Ethernet port is configured as a simulated member host, the simulated host sends an IGMP report through this port. Meanwhile, the simulated host sends the same IGMP report to itself and establishes a corresponding IGMP entry based on this report.
- When receiving an IGMP general query, the simulated host responds with an IGMP report. Meanwhile, the simulated host sends the same IGMP report to itself to ensure that the IGMP entry does not age out.
- When the simulated joining function is disabled on an Ethernet port, the simulated host sends an IGMP leave message.

Therefore, to ensure that IGMP entries will not age out, the port must receive IGMP general queries periodically.

Configuring IGMP Snooping simulated joining in VLAN interface view

Table 347 Configure IGMP Snooping simulated joining in VLAN interface view

Operation	Command	Description
Enter system view	**system-view**	-
Enter interface view	**interface Vlan-interface** *interface-number*	-
Configure one or more ports in the VLAN as simulated member host(s) of the specified multicast group	**igmp host-join** *group-address* [**source-ip** *source-address*] **port** *interface-list*	Optional Disabled by default

Configuring IGMP Snooping simulated joining in Ethernet port view

Table 348 Configure IGMP Snooping simulated joining in Ethernet port view

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Configure the port in the specified VLAN as a simulated member host of the specified multicast group	**igmp host-join** *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*	Optional Disabled by default



CAUTION:

- *Before configuring IGMP Snooping simulated joining, you must enable IGMP Snooping in VLAN interface view first.*

- *If you configure IGMP Snooping simulated joining in Ethernet port view, the Ethernet port must belong to the specified VLAN; otherwise the configuration does not take effect.*
- *You can use the **source-ip** source-address command to specify a multicast source address that the port will join as a simulated host. This configuration takes effect only when IMGPv3 Snooping is enabled in the VLAN.*

Configuring Multicast VLAN

In the current multicast mode, when users in different VLANs order the same multicast packet, the multicast stream is copied to each of the VLANs. This mode wastes a lot of bandwidth.

By configuring a multicast VLAN, adding switch ports to the multicast VLAN and enabling IGMP Snooping, you can make users in different VLANs share the same multicast VLAN. This saves bandwidth because multicast streams are transmitted only within the multicast VLAN and also guarantees security because the multicast VLAN is isolated from user VLANs completely. Therefore, multicast information streams can be transmitted to users continuously if multicast VLAN is configured.

Perform the following configuration to configure multicast VLAN.

Table 349 Configure multicast VLAN

Operation	Command	Description
Enter system view	**system-view**	-
Enable the IGMP snooping function globally	**igmp-snooping enable**	Required
Enter VLAN view	**vlan** *vlan-id*	-
Enable the IGMP snooping function	**igmp-snooping enable**	Required
Enable the multicast VLAN function	**multicast-vlan enable**	Required
Configure the mapping relationship between multicast VLAN and multicast sub-VLANs	**multicast-vlan** *vlan-id* **subvlan** *vlan-list*	Required

CAUTION:

- *You can configure up to 5 multicast VLANs for the device.*
- *A multicast VLAN cannot be configured as a multicast sub-VLAN.*
- *A multicast sub-VLAN cannot be configured as a multicast VLAN.*
- *A multicast sub-VLAN cannot be configured as the sub-VLAN of another multicast VLAN.*
- *A multicast sub-VLAN is corresponding to a multicast VLAN only.*
- *If multicast routing is enabled on a VLAN interface, the corresponding VLAN cannot be configured as a multicast VLAN.*

Displaying and Maintaining IGMP Snooping

After the configuration above, you can execute the **display** command to verify the configuration by checking the displayed information.

You can execute the **reset** command to clear the statistics information about IGMP Snooping.

Table 350 Display information about IGMP Snooping

Operation	Command	Description
Display the current IGMP Snooping configuration	**display igmp-snooping configuration**	You can execute the **display** commands in any view.
Display IGMP Snooping message statistics	**display igmp-snooping statistics**	
Display IP and MAC multicast groups in one or all VLANs	**display igmp-snooping group** [**vlan** *vlanid*]	
Display the configuration of the multicast VLAN	**display multicast-vlan** [*vlan-id*]	
Clear IGMP Snooping statistics	**reset igmp-snooping statistics**	You can execute the **reset** command in user view.

IGMP Snooping Configuration Example

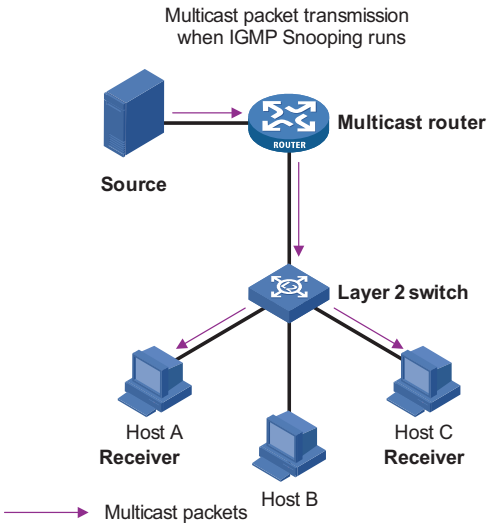
Configure IGMP Snooping on a switch

Network requirements

Connect the router port on the switch to the router, and other non-router ports which belong to VLAN 10 to user PCs. Enable IGMP Snooping on the switch.

Network diagram

Figure 108 Network diagram for IGMP Snooping configuration



Configuration procedure

Enable IGMP Snooping in system view.

```
<SW7750> system-view
[SW7750] igmp-snooping enable
```

Enable IGMP Snooping on VLAN 10.

```
[SW7750] vlan 10
[SW7750-vlan10] igmp-snooping enable
```

Configure Multicast VLAN

Network requirements

Table 351 lists all the devices in the network. Assume that port type configuration, VLAN division configuration, and IP address configuration for the interface are completed.

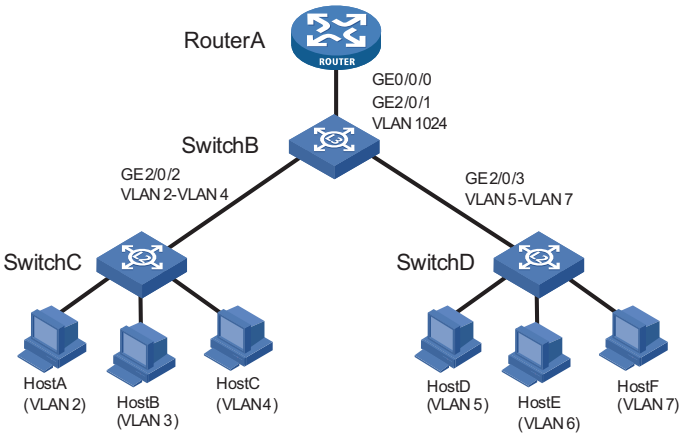
Table 351 List of network device configurations

Device ID	Device type	Port	Device connected to the port	Description
Router A	Router	GigabitEthernet 0/0/0	Switch B	GigabitEthernet0/0/0 belongs to VLAN1024, where the PIM-SM and IGMP protocols are enabled.
Switch B	Layer 3 switch	GigabitEthernet 2/0/1	Router A	GigabitEthernet 2/0/1 belongs to VLAN 1024.
		GigabitEthernet 2/0/2	Switch C	GigabitEthernet 2/0/2 is a trunk port belonging to VLAN 2 to VLAN 4.
		GigabitEthernet 2/0/3	Switch D	GigabitEthernet 2/0/3 is a trunk port belonging to VLAN 5 to VLAN 7.
Switch C	Layer 2 switch	The port connecting the upper-layer switch is configured as a trunk port.	-	Switch C is connected to users belonging to VLAN 2 to VLAN 4 where the IGMP snooping function is enabled.
Switch D	Layer 2 switch	The port connecting the upper-layer switch is configured as a trunk port.	-	Switch C is connected to users belonging to VLAN 5 to VLAN 7 where the IGMP snooping function is enabled.

Configure VLAN 1024 as a multicast VLAN and configure VLAN 2 to VLAN 7 as multicast sub-VLANs.

Network diagram

Figure 109 Network diagram for multicast VLAN configuration



Configuration procedure

Configure Router A.

```
<Router-A> system-view
[Router-A] multicast routing-enable
[Router-A] interface GigabitEthernet0/0/0
[Router-A-GigabitEthernet0/0/0] pim sm
[Router-A-GigabitEthernet0/0/0] igmp enable
[Router-A-GigabitEthernet0/0/0] quit
```

Configure Switch B.

```
<SW7750> system-view
[SW7750] igmp-snooping enable
[SW7750] vlan 1024
[SW7750-vlan1024]igmp-snooping enable
[SW7750-vlan1024] multicast-vlan enable
[SW7750-vlan1024] quit
[SW7750] multicast-vlan 1024 subvlan 2 to 7
```

Troubleshooting IGMP Snooping

Symptom: Multicast function does not work on the switch.

Solution:

The reason may be:

1. IGMP Snooping is not enabled.
   - Use the display current-configuration command to check the status of IGMP Snooping.
   - If IGMP Snooping is disabled, check whether it is disabled globally or on the corresponding VLAN. If it is disabled globally, use the igmp-snooping enable command in both system view and VLAN view to enable it both globally and on the corresponding VLAN at the same time. If it is only disabled on the corresponding VLAN, use the igmp-snooping enable command in VLAN view only to enable it on the corresponding VLAN.
2. Multicast forwarding table set up by IGMP Snooping is wrong.
   - Use the display igmp-snooping group command to check if the multicast groups are expected ones.
   - If the multicast group set up by IGMP Snooping is not correct, contact your technical support personnel.
   - Continue with solution 3) if the second step does not work.

If it is not the reason, the possible reason may be:

3. Multicast forwarding tables set up by IGMP Snooping is wrong.
   - Use the display mac-address vlan command to check whether the MAC multicast forwarding table set up in the vlan-id VLAN view is consistent with the one set up by IGMP Snooping.
   - If they are not consistent, contact your technical support personnel.

44 COMMON MULTICAST CONFIGURATION

Overview

Common multicast configuration tasks are the common contents of multicast group management protocol and multicast routing protocol. You must enable the common multicast configuration on the switch before enabling the two protocols.

Common multicast configuration includes:

- Configuring limit on the number of route entries: when the multicast routing protocol is configured on the switch, plenty of multicast route entries will be sent to upstream Layer 3 switches or routers. In order to prevent plenty of multicast route entries from consuming all the memory of the Layer 3 switches or routers, you can configure limit on the number of route entries to prevent too many route entries from being sent to Layer 3 switches or routers.
- Configuring suppression on the multicast source port: In the network, some users may set up multicast servers privately, which results in the shortage of multicast network resources and affects the multicast bandwidth and the transmission of valid information in the network. You can configure the suppression on the multicast source port feature to filter multicast packets on the unauthorized multicast source port, so as to prevent the users connected to the port from setting up multicast servers privately.
- Clearing the related multicast entries: through clearing the related multicast entries, you can clear the multicast route entries saved in the memory of the Layer 3 switches or routers to release the system memory

Common Multicast Configuration Tasks

Table 352 Common multicast configuration tasks

Operation	Description	Related section
Enable multicast routing and configure limit on the number of multicast route entries	Required	"Enabling Multicast Routing and Configuring Limit on the Number of Multicast Route Entries" on page 442
Configure suppression on the multicast source port	Optional	"Configuring Suppression on the Multicast Source Port" on page 442
Configure suppression on multicast wrongif packets	Optional	"Configuring Suppression on Multicast Wrongif Packets" on page 442
Configure static router ports	Optional	"Configuring Static Router Ports" on page 443
Clear the related multicast entries	Optional	"Clearing the Related Multicast Entries" on page 444

Enabling Multicast Routing and Configuring Limit on the Number of Multicast Route Entries

Table 353 Enable multicast routing and configure limit on the number of multicast route entries

Operation	Command	Description
Enter system view	**system-view**	-
Enable multicast routing	**multicast routing-enable**	Required Multicast routing must be enabled before the multicast group management protocol and the multicast routing protocol are configured.
Configure limit on the number of multicast route entries	**multicast route-limit** *limit*	Optional By default, the limit on the number of multicast route entries is 1,024.

CAUTION: *The other multicast configurations do not take effect until multicast routing is enabled.*

Configuring Suppression on the Multicast Source Port

Configuring suppression on the multicast source port in system view

Table 354 Configure suppression on the multicast source port

Operation	Command	Description
Enter system view	**system-view**	-
Configure suppression on the multicast source port	**multicast-source-deny enable** [**interface** *interface-list*]	Required The suppression on the multicast source port feature is disabled by default.

Configuring suppression on the multicast source port in Ethernet port view

Table 355 Configure suppression on the multicast source port

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Configure suppression on the multicast source port	**multicast-source-deny enable**	Optional The suppression on the multicast source port feature is disabled by default.

CAUTION: *The following I/O Modules do not support the suppression on the multicast source port feature: 3C16860, 3C16861, LS81FS24A, 3C16859, and 3C16858.*

Configuring Suppression on Multicast Wrongif Packets

Introduction

When the switch receives a multicast packet, the switch will search the multicast forwarding entry according to the source address and destination address of the packet. If the matching forwarding entry is found and the packet is received on the right ingress of the forwarding entry, the packet will be forwarded according

to the forwarding entry. If the packet is not received on the right ingress of the forwarding entry, the packet is regarded as a wrongif packet. The wrongif packet will be reported to the CPU for processing.

In some network, many wrongif packets will be reported to the CPU of the switch for processing, thus aggravating the workload of the switch. In this case, you can configure suppression on the holdtime of wrongif packets, so that the wrongif packets will be dropped instead of being forwarded to the CPU of the switch for processing, and the CPU will be prevented from being stricken by too many packets.

Table 356 Configure suppression on the holdtime of multicast wrongif packets

Operation	Command	Description
Enter system view	**system-view**	-
Configure suppression on the holdtime of multicast wrongif packets	**multicast wrongif-holdtime** *seconds*	Required By default, the holdtime of multicast wrongif packets is 15 seconds.

CAUTION:

- *During the configuration, if the seconds argument is less than 15, the system sets the holdtime to 15; if the seconds argument is more than 15, the system sets the holdtime to the multiples of 15 according to the user-defined range. For example, if you set the seconds argument to 14, the system sets the holdtime to 15; if you set the seconds argument to 16, the system sets the holdtime to 30; if you set the seconds argument to 31, the system sets the holdtime to 45, and so on.*
- *When the holdtime is set to 0, the report of CPU packets to the CPU is not suppressed.*

Configuring Static Router Ports

In a ring network or a network with double uplinks, users usually configure both primary and secondary links over a connection in order to avoid communication interruption due to link failure. When the primary link fails, the secondary link can replace it immediately to avoid communication interruption.

On a link where a multicast protocol (such as PIM or IGMP) is enabled, the switch cannot restore multicast data transmission after switchover until the switch receives multicast packets (such as PIM Hello packets and IGMP general group query messages) and adds the static router port to the corresponding multicast entry. The process will cause temporary interruption of multicast data transmission. For real-time services such as IPTV, the delay will cause some undesirable problems such as picture jitter.

You can configure a port as a static router port. When the link state switches, the multicast data can be switched from the primary link to the secondary link immediately, so that the switch need not wait for multicast protocol packets and the multicast data transmission delay is avoided. Additionally, a static port never times out except when a link fails or the configuration is removed.

Configure static router ports as follows:

- Enable IGMP snooping globally
- Enable multicast routing globally
- Allocate an Ethernet port to the corresponding VLAN
- Configure an IP address for the VLAN
- Enable the multicast routing protocol on the VLAN interface
- Bring the Ethernet port to the up state

Configuring static router ports in Ethernet port view

Table 357 Configure static router ports

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Configure static router ports	**multicast static-router-port vlan** *vlan-id*	Required

Configuring static router ports in VLAN view

Operation	Command	Description
Enter system view	**system-view**	-
Enter VLAN view	**vlan** *vlan-id*	-
Configure static router ports	**multicast static-router-port interface** *interface-type interface-number*	Required

CAUTION: *You can configure static router ports in Ethernet port view or VLAN view, but you can view the related configuration information in Ethernet port view only.*

Clearing the Related Multicast Entries

Use the **reset** command in user view to clear the related statistics information about the common multicast configuration.

Table 358 Clear the related multicast entries

Operation	Command	Description
Clear the multicast forwarding case (MFC) forwarding entries or statistics information about the forwarding entries	**reset multicast forwarding-table** [**statistics**] { **all** | { *group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }] | **incoming-interface** *interface-type interface-number* } * }	Clear the related MFC forwarding entries
Clear the route entries in the core multicast routing table	**reset multicast routing-table** { **all** | { *group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }] | { **incoming-interface** *interface-type interface-num*ber } } * }	Clear the route entries in the core multicast routing table

Displaying Common Multicast Configuration

After the configuration above, you can execute the **display** command to verify the configuration by checking the displayed information.

The multicast forwarding table is mainly used for debugging. Generally, you can get the required information by checking the core multicast routing table.

Table 359 Display common multicast configuration

Operation	Command	Description
Display the statistics information about the suppression on the multicast source port	**display multicast-source-deny** [**interface** *interface-type* [*interface-number*]]	You can execute the **display** commanding any view. ■ If neither the port type nor the port number is specified, the statistics information about the suppression on all the multicast source ports on the switch is displayed. ■ If only the port type is specified, the statistics information about the suppression on the multicast source ports of the type is displayed. ■ If both the port type and the port number is specified, the statistics information about the suppression on the specified multicast source port is displayed.

Table 359 Display common multicast configuration

Operation	Command	Description
Display the information about the multicast routing table	**display multicast routing-table** [*group-address* [**mask** { *group-mask* | *mask-length* }] | *source-address* [**mask** { *group-mask* | *mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** }]*	You can execute the **display** commanding any view.
Display the information about the multicast forwarding table	**display multicast forwarding-table** [*group-address* [**mask** { *group-mask* | *mask-length* }] | *source-address* [**mask** { *group-mask* | *mask-length* }] | **incoming-interface** { *interface-type interface-number*] **register** }]*	
Display the information about the multicast forwarding tables containing port information	**display mpm forwarding-table** [*group-address*]	
Display the information about IP multicast groups and MAC multicast groups in one VLAN or all the VLANs on the switch	**display mpm group** [**vlan** *vlan-id*]	

Three kinds of tables affect data transmission. The correlations of them are:

- Each multicast routing protocol has its own multicast routing table.
- The multicast routing information of all multicast routing protocols is integrated to form the core multicast routing table.
- The core multicast routing table is consistent with the multicast forwarding table, which is in really in charge of multicast packet forwarding.

45 STATIC MULTICAST MAC ADDRESS TABLE CONFIGURATION

Overview

In Layer 2 multicast, the system can add multicast forwarding entries dynamically through Layer 2 multicast protocol. However, you can also statically bind a port to a multicast address entry by configuring a multicast MAC address entry manually.

Generally, when receiving a multicast packet whose multicast address has not yet been registered on the switch, the switch will broadcast the packet in the VLAN to which the port belongs. However, you can configure a static multicast MAC address entry to avoid this case.

Configuring a Multicast MAC Address Entry

Table 360 Configure a multicast MAC address entry

Operation	Command	Description
Enter system view	**system-view**	-
Create a multicast MAC address entry	**mac-address multicast** *mac-address* **interface** *interface-list* **vlan** *vlan-id*	Required The *mac-address* argument must be a multicast MAC address The *vlan-id* argument is the ID of the VLAN to which the port belongs



- *If the multicast MAC address entry to be created already exists, the system gives you a prompt.*
- *If a multicast MAC address is added manually, the switch will not learn this multicast MAC address again through IGMP Snooping. The **undo mac-address multicast** command is used to delete the multicast MAC address entries created by the **mac-address multicast** command manually, however, it cannot be used to delete the multicast MAC address entries learned by the switch.*
- *If you want to add a port to a multicast MAC address entry created through the **mac-address multicast** command, you must delete this entry first, create this entry again, and then add the specified port to the forwarding ports of this entry.*
- *You cannot enable port aggregation on a port where you have configured a multicast MAC address; and you cannot configure a multicast MAC address on an aggregation port.*

Displaying Multicast MAC Address

After the configuration above, you can execute the **display** command to verify the configuration effect by checking the displayed information.

Table 361 Display the multicast MAC addresses

Operation	Command	Description
Display the static multicast MAC addresses	**display mac-address multicast** [**count**]	You can use the **display** command in any view.

46 IGMP CONFIGURATION

Overview

Introduction to IGMP

Internet group management protocol (IGMP) is responsible for the management of IP multicast members. It is used to establish and maintain membership between IP hosts and their directly connected neighboring routers.

The IGMP feature does not transmit and maintain the membership information among multicast routers. This task is completed by multicast routing protocols. All the hosts participating in multicast must support the IGMP feature.

IGMP is divided into two function parts:

- Host side: the hosts participating IP multicast can join or exit a multicast group anywhere and anytime.
- Router side: through the IGMP protocol, a multicast router checks the network segment connected with each interface to see whether there are receivers of a multicast group, namely, group members.

A multicast router need not and cannot save the membership information of all the hosts. While, a host has to save the information that which multicast groups that it joins in.

IGMP is asymmetric between the host and the router. The host needs to respond to the IGMP query messages of the multicast routers, that is, report message responses as an IGMP host. The multicast router sends IGMP general query messages periodically and determines whether any host of a specified group joins in its subnet based on the received response packets. When the router receives IGMP leave messages, it will send IGMPv2 group-specific query messages to find out whether the specified group still has any member.

IGMP Version

IGMP has three versions until now, including: IGMP Version 1 defined by RFC1112, IGMP Version 2 defined by RFC2236 and RFC Version 3. IGMP Version 2 is the most widely used currently.

Compared with IGMP Version 2, the advantages of IGMP Version 2 are:

Multicast router election mechanism on a shared network segment

A shared network segment is a network segment with multiple multicast routers. In this case, all routers running IGMP on this network segment can receive the membership report messages from hosts. Therefore, only one router is necessary to send membership query messages. In this case, the querier selection mechanism is required to specify a router as the querier.

In IGMP Version 1, the multicast routing protocol selects the querier. In IGMP Version 2, it is defined that the multicast router with the lowest IP address is selected as the querier when there are multiple multicast routers in a network segment.

Leave group mechanism

In IGMP Version 1, hosts leave the multicast group quietly without informing any multicast router. Only when a query message times out can the multicast router know that a host has left the group. In IGMP Version 2, when a host replying to the last membership query message decides to leave a multicast group, it will send a leave group message to the multicast router.

Group-specific query

In IGMP Version 1, a multicast query message of the multicast router aims at all the multicast groups in the network segment. This query is called general query.

IGMP version 2 adds group-specific query, where the IP address of a multicast group is taken as the destination IP address and the group address field of the query message, to prevent the member hosts of other groups from responding to this message.

Maximum response time

The Maximum Response Time field is added in IGMP Version 2. It is used to dynamically adjust the maximum time for a host to respond to the membership query message.

Working Procedure of IGMP

The working procedure of IGMP is as follows:

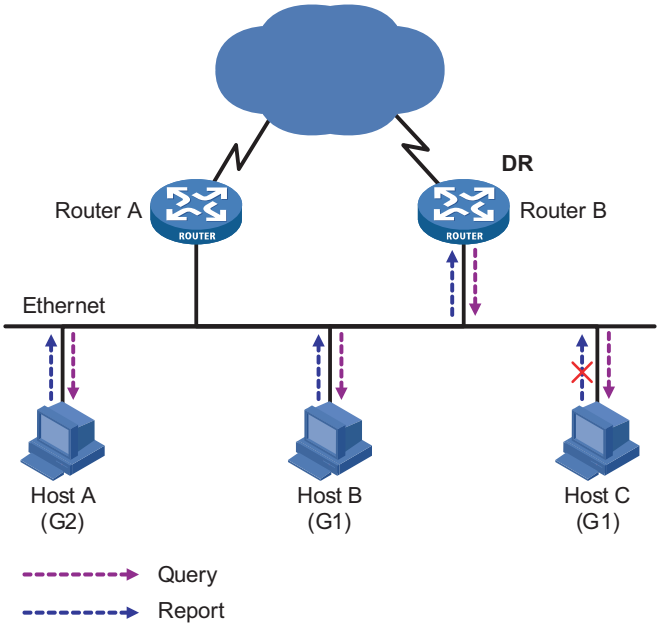
- The receiver host reports the membership to its shared network.
- A querier (IGMPv2) is selected from all the IGMP-enabled routers in the same network segment.
- The querier periodically sends group member query messages to the shared network segment.
- The receiver host responds to the received query message to report the group membership.
- The querier refreshes the presence information of the group members according to the received responses.

All the receiver hosts participating in multicast transmission must support the IGMP protocol. The multicast router need not and cannot save the membership information of all the hosts. It checks the network segment connected with each interface by IGMP to see whether there are receivers of a multicast group, namely, group members. While each host saves only the information that which multicast groups it joins.

Working mechanism of IGMPv1

IGMPv1 protocol (RFC1112) manages the multicast groups based on the query/response mechanism. With the help of the Layer 3 routing protocol, IGMP selects the designated router (DR) as the querier, which is responsible for sending query messages. Figure 110 describes the IGMPv1 message interaction in the network:

Figure 110 Working mechanism of IGMPv1



A host joins in the multicast group in the following procedure:

- The IGMP querier (such as DR) periodically multicasts IGMP general group query messages to all the hosts in the shared network segment whose address is 224.0.0.1.
- All hosts in the network receive the query messages. If some hosts (such as Host B and Host C) are interested in the multicast group G1, Host B and Host C will multicast IGMP host report messages (carrying the address of the multicast group G1) to declare that they will join in the multicast group G1.
- All the hosts and routers in the network receive the IGMP host report messages and get to know the address of the multicast group G1. In this case, if other hosts in the network want to join in the multicast group G1, they will not send IGMP host report messages about G1. If some hosts in the network want to join in another multicast group G2, they will send IGMP host report messages about G2 to respond to the query messages.
- After the query/response process, the IGMP routers get to know that receivers corresponding to the multicast group G1 exist in the network, and generate the (*, G1) multicast forwarding entries, according to which the multicast information is forwarded.
- The data from the multicast source reaches the IGMP router through the multicast routes. If there are receivers in the network connected to the IGMP router, the data will be forwarded to this network segment and the receiver hosts receive the data.

IGMP leave packet is not defined in IGMPv1, so when a host leaves a multicast group, only when a query message times out can the multicast router know that a host has left the group.

When all the hosts in a network segment have left the multicast group, the branch corresponding to the related network segment is pruned from the multicast tree.

Enhancements Provided by IGMPv2

Compared with IGMPv1, IGMPv2 provides the querier election mechanism and Leave Group mechanism.

- Querier election mechanism

In IGMPv1, the DR elected by the Layer 3 multicast routing protocol (such as PIM) serves as the querier among multiple routers on the same subnet.

In IGMPv2, an independent querier election mechanism is introduced. The querier election process is as follows:

1. Initially, every IGMPv2 router assumes itself as the querier and sends IGMP general query messages (often referred to as general queries) to all hosts and routers on the local subnet (the destination address is 224.0.0.1).
2. Upon hearing a general query, every IGMPv2 router compares the source IP address of the query message with its own interface address. After comparison, the router with the lowest IP address wins the querier election and all other IGMPv2 routers become non-queriers.
3. All the non-queriers start a timer, known as "other querier present timer". If a router receives an IGMP query from the querier before the timer expires, it resets this timer; otherwise, it assumes the querier to have timed out and initiates a new querier election process.

- Leave group" mechanism

In IGMPv1, when a host leaves a multicast group, it does not send any notification to the multicast router. The multicast router relies on IGMP query response timeout to know whether a group no longer has members. This adds to the leave latency.

In IGMPv2, on the other hand, when a host leaves a multicast group:

1. This host sends a Leave Group message (often referred to as leave message) to all routers (the destination address is 224.0.0.2) on the local subnet.
2. Upon receiving the leave message, the querier sends a configurable number of group-specific queries to the group being left. The destination address field and group address field of message are both filled with the address of the multicast group being queried.
3. One of the remaining members, if any on the subnet, of the group being queried should send a membership report within the maximum response time set in the query messages.

If the querier receives a membership report for the group within the maximum response time, it will maintain the memberships of the group; otherwise, the querier will assume that no hosts on the subnet are still interested in multicast traffic to that group and will stop maintaining the memberships of the group.

IGMP Proxy

A lot of leaf networks (leaf domains) are involved in the application of a multicast routing protocol (PIM-DM for example) over a large-scaled network. It is a hard work to configure and manage these leaf networks.

To reduce the workload of configuration and management without affecting the multicast connection of leaf networks, you can configure an IGMP Proxy in a Layer

3 switch in the leaf network (Switch B in the figure). The Layer 3 switch will then forward IGMP join or IGMP leave messages sent by the connected hosts. After the configuration of IGMP Proxy, the leaf switch is no longer a PIM neighbor but a host for the external network. Only when the Layer 3 switch has directly connected members, can it receive the multicast data of corresponding groups.

Figure 111 Diagram for IGMP Proxy

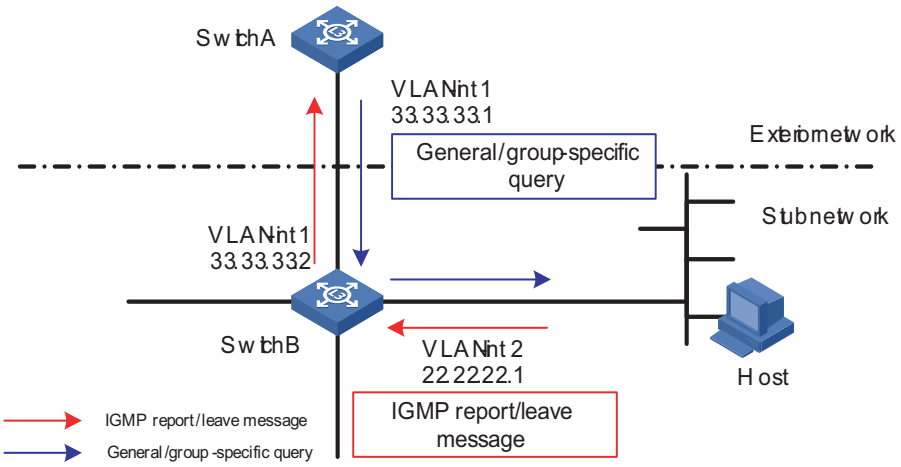


Figure 111 is an IGMP Proxy diagram for a leaf network.

Configure Switch B as follows:

- Enable multicast routing on VLAN interface 1 and VLAN interface 2, and then configure the PIM protocol on it. And configure the IGMP protocol on VLAN-interface 1 at the same time.
- On VLAN interface 2, configure VLAN interface 1 as the outbound IGMP Proxy interface to external networks. You must enable the IGMP protocol on the interface first, and then configure the igmp proxy command.

Configure Switch A as follows:

- Enable multicast routing and configure the IGMP protocol on VLAN interface 1.
- Configure the pim neighbor-policy command to filter PIM neighbors in the network segment 33.33.33.0/24. That is, Switch A does not consider Switch B as its PIM neighbor.

In this case, when Switch B of leaf network receives from VLAN interface 2 an IGMP join or IGMP leave message sent by the host, it will change the source address of the IGMP information to the address of VLAN interface 1: 33.33.33.2 and send the information to VLAN interface 1 of Switch A. For Switch A, this works as if there is a host directly connected to VLAN interface 1.

Similarly, when Switch B receives the IGMP general group or group-specific query message from the Layer 3 Switch A, it will also change the source address of the query message to the IP address of VLAN interface 2: 22.22.22.1 and send the message from VLAN interface 2.

In Figure 111, VLAN interface 2 of Switch B is called the client and VLAN interface 1 of Switch B is called the proxy.

IGMP Configuration Tasks

Table 362 Configuration task overview

Operation	Description	Related section
Configure IGMP version	Optional	"Configuring IGMP Version" on page 454
Configure IGMP query messages	Optional	"Configuring IGMP Query Packets" on page 454
Configure IGMP multicast groups on the interface	Optional	"Configuring IGMP Multicast Groups on the Interface" on page 456
Configure IGMP simulated joining	Optional	"Configuring IGMP Simulated Joining" on page 458
Configure IGMP Proxy	Optional	"Configuring IGMP Proxy" on page 459
Configure suppression on IGMP host report messages	Optional	"Configuring Suppression on IGMP Host Report Messages" on page 459
Remove the joined IGMP groups from the interface	Optional	"Removing the Joined IGMP Groups from the Interface" on page 460

Configuring IGMP Version

Table 363 Configure IGMP version

Operation	Command	Description
Enter system view	**system-view**	-
Enable the multicast routing protocol	**multicast routing-enable**	Enable the multicast routing protocol
Enter VLAN interface view	**interface vlan-interface** *interface-number*	-
Enable IGMP on the current interface	**igmp enable**	Required By default, if IP multicast routing is enabled globally, IGMP is enabled on all the layer-3 interfaces automatically.
Configure the IGMP version of the Layer 3 switch (router)	**igmp version** { **1** | **2** }	Optional IGMP version 2 is used by default.



CAUTION: *Each IGMP version cannot be switched to each other automatically. So all the Layer 3 switches on a subnet must be configured to use the same IGMP version.*

Configuring IGMP Query Packets

IGMP general query messages

The Layer 3 switch sends IGMP general query messages to the connected network segment periodically to get to know which multicast groups in the network segment have members according to the returned IGMP report messages. The multicast router also sends query messages periodically. When it receives the IGMP join messages of a group member, it will refresh the membership information of the network segment.

IGMP group-specific query messages

The query router (querier for short) maintains the IGMP join messages on the interface on the shared network. After the related features are configured, the IGMP querier will send IGMP group-specific query messages at the user-defined interval for the user-defined times when it receives the IGMP leave messages from the hosts.

Suppose a host in a multicast group decides to leave the multicast group. The related procedure is as follows:

- The host sends an IGMP leave packet.
- When the IGMP querier receives the packet, it will send IGMP group-specific query messages at the interval configured by the igmp **lastmember-queryinterval** command (the interval is 1 second by default) for the robust-value times (the robust-value argument is configured by the igmp robust-count command and it is 2 by default).
- If other hosts are interested in the group after receiving the IGMP group-specific query message from the querier, they will send IGMP join messages in the maximum response time specified in the packet.
- If the IGMP querier receives IGMP join messages from other hosts within the robust-value x seconds time, it will maintain the membership of the group.
- If the IGMP querier does not receive IGMP join messages from other hosts after the robust-value x seconds time, it considers the group times out and will not maintain the membership of the group.

The procedure is only fit for the occasion when IGMP queriers runs IGMP version 2.

If the host runs IGMP version 1, it does not send IGMP leave messages when leaving a group, so the conditions will be the same as described in the procedure above.

IGMP querier substitution rules

The lifetime of an IGMP querier is limited. If the former querier does not send query messages in the specified time, another router will replace the IGMP querier.

The maximum query time of IGMP packets

When the host receives a query message, it will set a timer for each of its multicast groups. The timer value is selected from 0 to the maximum response time at random. When the value of a timer decreases to 0, the host will send the membership information of the multicast group.

Through configuring the reasonable maximum response time, you can enable the host to respond to the query information quickly and enable the Layer 3 switch to understand the membership information of multicast groups quickly.

Table 364 Configure IGMP query messages

Operation	Command	Description
Enter system view	**system-view**	-

Table 364 Configure IGMP query messages

Operation	Command	Description
Enable the multicast routing protocol	**multicast routing-enable**	Required
Enter VLAN interface view	**interface Vlan-interface** *interface-number*	-
Enable IGMP on the current interface	**igmp enable**	Required By default, if the IP multicast routing protocol is enabled globally, IGMP is enabled on all the layer-3 interfaces automatically.
Configure the query interval	**igmp timer query** *seconds*	Optional The query interval is 60 seconds by default.
Configuring the interval of sending IGMP group-specific query messages	**igmp lastmember-queryinterval** *seconds*	Optional By default, the interval of sending IGMP group-specific query messages is 1 second.
Configuring the times of sending IGMP group-specific query messages	**igmp robust-count** *robust-value*	Optional By default, the times of sending IGMP group-specific query messages is 2.
Configure the maximum lifetime of an IGMP querier	**igmp timer other-querier-present** *seconds*	Optional ■ The lifetime of an IGMP querier is 120 seconds by default. ■ If the Layer 3 switch does not receive query messages in two times of the interval specified by the **igmp timer query** command, the former querier is considered as ineffective.
Configure the maximum IGMP query response time	**igmp max-response-time** *seconds*	Optional The maximum IGMP query response time is 10 seconds.

CAUTION: *When there are multiple multicast routers in a network segment, the querier is responsible for sending IGMP query messages to all the hosts in the network segment.*

Configuring IGMP Multicast Groups on the Interface

You can perform the following configurations on the interface for the IGMP multicast groups:

- Limit the number of multicast groups
- Limit the range of multicast groups that the interface serves

Limiting the number of joined multicast groups

If the number of joined IGMP groups on the multicast routing interface of the switch is not limited, the memory of the switch may be used out and the routing

interface of the switch may fail when plenty of multicast groups join in the routing interface.

You can configure limit on the number of IGMP multicast groups on the interface of the switch. Thus, when users are ordering the programs of multicast groups, the network bandwidth can be controlled because the number of multicast groups is limited.

Limiting the range of multicast groups that the interface serves

The Layer 3 switch determines the membership of the network segment through translating the received IGMP join messages. You can configure a filter for each interface to limit the range of multicast groups that the interface serves.

Table 365 Configure IGMP multicast groups on the interface

Operation	Command	Description
Enter system view	**system-view**	-
Enable the multicast routing protocol	**multicast routing-enable**	Required
Enter VLAN interface view	**interface Vlan-interface** *interface-number*	-
Enable IGMP on the current interface	**igmp enable**	By default, if the IP multicast routing protocol is enabled globally, IGMP is enabled on all the layer-3 interfaces automatically.
Configure limit on the number of IGMP groups on the interface	**igmp group-limit** *limit*	Optional By default, the number of multicast groups on a VLAN interface is 256.
Limit the range of multicast groups that the interface serves	**igmp group-policy** *acl-number* [**1** | **2** | **port** *interface-type interface-number* [**to** *interface-type interface-number*]]	Optional ■ By default, the filter is not configured, that is, any multicast group is permitted on a port. ■ If the **port** keyword is specified, the specified port must belong to the VLAN of the VLAN interface. ■ You can configure to filter the IP addresses of some multicast groups in ACL. ■ 1 and 2 are the IGMP version numbers. IGMPv2 is used by default.
Quit interface view.	**quit**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-

Table 365 Configure IGMP multicast groups on the interface

Operation	Command	Description
Limit the range of multicast groups that the interface serves	**igmp group-policy** *acl-number* **vlan** *vlan-id*	Optional ■ By default, the filter is not configured, that is, any multicast group is permitted on the port. ■ The port must belong to the IGMP-enabled VLAN specified in the command. Otherwise, the command does not take effect.

CAUTION:

- *If the number of joined multicast groups on the interface exceeds the user-defined limit, new groups are not allowed to join any more.*
- *If the number of existing IGMP multicast groups has exceeded the configured limit on the number of joined multicast groups on the interface, the system will delete some existing multicast groups automatically until the number of multicast groups on the interface is conforming to the conferred limit.*

Configuring IGMP Simulated Joining

Simulated joining in IGMP is implemented in the same way as in IGMP Snooping except that IGMP establishes and maintains IGMP entries.

Enabling IGMP simulated joining in interface view

Table 366 Enable IGMP simulated joining in interface view

To do...	Use the command...	Description
Enter system view	**system-view**	-
Enter VLAN interface view	**interface Vlan-interface** *interface-number*	-
Enable simulated joining	**igmp host-join** *group-address* **port** *interface-list*	Optional Disabled by default

Configuring IGMP simulated joining in Ethernet port view

Table 367 Configure IGMP simulated joining on a port

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Configure IGMP simulated joining	**igmp host-join** *group-address* **vlan** *vlan-id*	Optional Simulated joining is disabled by default.

CAUTION:

- *Before configuring IGMP simulated joining, enable IGMP in interface view first.*

- *If you configure IGMP simulated joining in Ethernet port view, the port to be configured must belong to the specified VLAN; otherwise the configuration does not take effect.*

Configuring IGMP Proxy

Configuring IGMP proxy

You can configure IGMP proxy to reduce the workload of configuration and management of leaf networks without affecting the multicast connections of the leaf network.

After the configuration of IGMP Proxy on the Layer 3 switch of the leaf network, the leaf Layer 3 switch is just a host for the external network. Only when the Layer 3 switch has directly connected members, can it receive the multicast data of corresponding groups.

Table 368 Configure IGMP proxy

Operation	Command	Description
Enter system view	**system-view**	-
Enable the multicast routing protocol	**multicast routing-enable**	Required
Enter VLAN interface (which is connected to the external network) view	**interface Vlan-interface** *interface-number*	-
Enable PIM-DM on this interface	**pim dm**	-
Enable the IGMP protocol	**igmp enable**	Required By default, if the IP multicast routing protocol is enabled globally, IGMP is enabled on all the layer-3 interfaces automatically.
Configure IGMP Proxy	**igmp proxy Vlan-interface** *interface-number*	Required By default, the IGMP Proxy feature is disabled.

CAUTION:

- *Both the multicast routing protocol and the IGMP protocol must be enabled on the proxy interface.*
- *You must enable PIM DM on the interface before configuring the* ***igmp proxy*** *command. Otherwise, the IGMP Proxy feature does not take effect.*
- *Only one IGMP proxy interface can be configured for one interface.*

Configuring Suppression on IGMP Host Report Messages

When a Layer 2 switch receives an IGMP host report message from a host in a multicast group, the switch will forward the message to the Layer 3 switch port connecting to it. If there are multiple hosts in a multicast group, the Layer 3 switch will receive the same IGMP host report messages from multiple hosts in a multicast group.

When the suppression on IGMP host report messages is enabled, the Layer 3 switch will receive only the first IGMP host report message from the hosts in a

multicast group and drop the other IGMP host report messages from the multicast group.

Table 369 Configure suppression on IGMP host report messages

Operation	Command	Description
Enter system view	**system-view**	-
Configure suppression on IGMP host report messages	**igmp report-aggregation**	Required By default, the suppression on IGMP host report messages is disabled.

Removing the Joined IGMP Groups from the Interface

You can remove all the joined IGMP groups on all ports of the router or all the joined IGMP groups on the specified interfaces, or remove a specified IGMP group address or group address network segment on the specified interface.

Table 370 Remove the joined IGMP groups from the interface

Operation	Command	Description
Remove the joined IGMP groups from the interface	**reset igmp group** { **all** | **interface** *interface-type interface-number* { **all** | *group-address* [*group-mask*] } }	Optional

CAUTION: *When an IGMP group is removed from an interface, the IGMP group can join the group again.*

Displaying IGMP

After completing the above configurations, you can execute the **display** command to verify the configuration by checking the displayed information.

Table 371 Display IGMP

Operation	Command	Description
Display the membership information of the IGMP multicast group	**display igmp group** [*group-address* | **interface** *interface-type interface-number*]	You can execute the **display** command in any view.
Display the IGMP configuration and running information of the interface	**display igmp interface** [*interface-type interface-number*]	

47 PIM CONFIGURATION

PIM Overview

Protocol independent multicast (PIM) means that the unicast routing protocols providing routes for the multicast could be static routes, RIP, OSPF, IS-IS, or BGP. The multicast routing protocol is independent of unicast routing protocols only if unicast routing protocols can generate route entries.

With the help of the reverse path forwarding, PIM can transmit multicast information in the network. For the convenience of description, the network consisted of PIM-enabled multicast routers is called PIM multicast domain.

Introduction to PIM-DM

Protocol independent multicast dense mode (PIM-DM) is a dense mode multicast protocol. It is suitable for small networks.

The features of such network are:

- Members in a multicast group are dense.
- PIM-DM assumes that in each subnet of the network there is at least one receiver interested in the multicast source.
- Multicast packets are flooded to all the points in the network, and the related resources (bandwidth and the CPU of the router) are consumed at the same time.

In order to reduce the network resource consumption, PIM-DM prunes the branches which do not forward multicast data and keeps only the branches including receivers. In order that the pruned branches which are demanded to forward multicast data can receive multicast data flows again, the pruned branches can be restored to the forwarding status periodically.

In order to reduce the delay time for a pruned branch to be restored to the forwarding status, PIM-DM uses the graft mechanism to restore the multicast packet forwarding automatically. Such periodical floods and prunes are the features of PIM-DM, which is suitable for small LANs only. The flood-prune" technology adopted in PIM-DM is unacceptable in WAN.

Generally, the packet forwarding path in PIM-DM is a shortest path tree (SPT) with the multicast source as the root and multicast members as the leaves. The SPT uses the shortest path from the multicast source to the receiver.

Work Mechanism of PIM-DM

The working procedure of PIM-DM is summarized as follows:

- Neighbor discovery
- SPT establishing
- Graft

- RPF check
- Assert mechanism

Neighbor discovery

In PIM-DM network, the multicast router needs to use Hello messages to perform neighbor discovery and maintain the neighbor relation when it is started. All routers keep in touch with each other through sending Hello messages periodically, and thus SPT is established and maintained.

SPT establishment

The procedure of establishing SPT is also called Flooding&Prune.

The procedure is as follows:

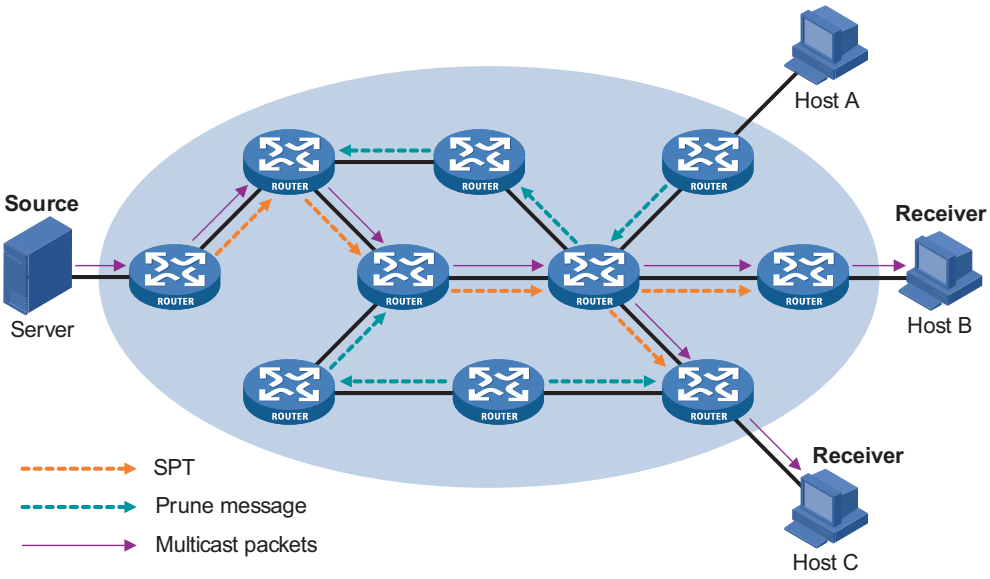
- PIM-DM assumes that all hosts on the network are ready to receive multicast data.
- When a multicast router receives a multicast packet from a multicast source "S" to a multicast group "G", it begins with RPF check according to the unicast routing table.
- If the RPF check passes, the router will create an entry(S, G) and forward the packet to all the downstream PIM-DM nodes. That is the process of flooding.
- If not, that is, the router considers that the multicast packets travel into the router through incorrect interfaces, the router just discards the packets.

After this process, the router will create a (S, G) entry for every host in PIM-DM domain.

If there is no multicast group member in the downstream nodes, the router will send a prune message to the upstream nodes to inform them not to forward data any more. The upstream nodes, as informed, will remove the relative interface from the outgoing interface list corresponding to the multicast forwarding entry (S, G). The pruning process continues until there are only necessary branches in PIM-DM. In this way, a SPT (Shortest Path Tree) rooted at source S is established.

The pruning process is initiated by leaf routers. As shown in Figure 112, the routers without receivers (such as the router connected to User A) initiates the pruning process automatically.

Figure 112 Diagram for SPT establishment in PIM-DM



The process above is called "Flooding and Pruning". Every pruned node also provides timeout mechanism. If pruning behavior times out, the router will initiate another flooding and pruning process. This process is performed periodically for PIM-DM.

Graft

When a pruned downstream node needs to be restored to the forwarding state, it may send a graft packet to inform the upstream node. As shown in Figure 113, user A receives multicast data again. Graft messages will be sent hop by hop to the multicast source S. The intermediate nodes will return acknowledgements when receiving Graft messages. Thus, the pruned branches are restored to the information transmission state.

RPF check

PIM-DM adopts the RPF check mechanism to establish a multicast forwarding tree from the data source S based on the existing unicast routing table, static multicast routing table, and MBGP routing table.

The procedure is as follows:

- When a multicast packet arrives, the router first checks the path.
- If the interface this packet reaches is the one along the unicast route towards the multicast source, the path is considered as correct.
- Otherwise, the multicast packet will be discarded as a redundant one.

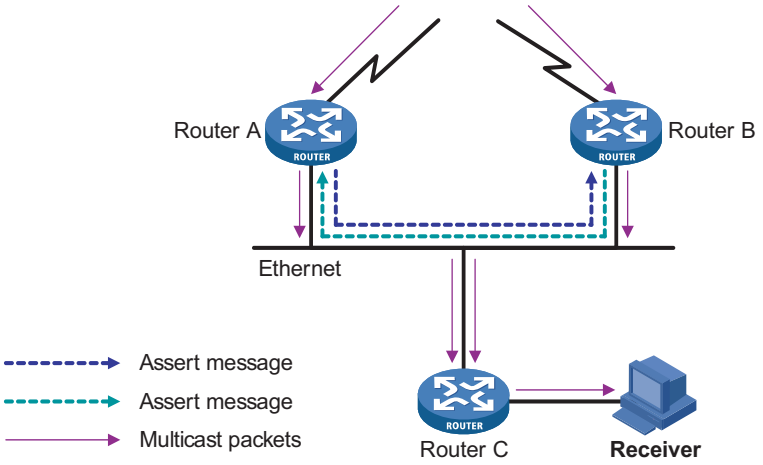
The unicast routing information on which the path judgment is based can be of any unicast routing protocol such as RIP or OSPF. It is independent of the specified unicast routing protocol. The static multicast routing table needs to be configured manually, and the MBGP routing table is provided by the MBGP protocol.

When multiple equivalent routes exit, the RPF check mechanism selects the upstream interface with the highest IP address as the incoming interface for the packet.

Assert mechanism

In the shared network such as Ethernet, the same packets may be sent repeatedly. For example, the LAN network segments contains many multicast routers, A, B, C, and D. They each have their own receiving path to the multicast source S. As shown in Figure 113:

Figure 113 Diagram for assert mechanism



When Router A, Router B, and Router C receive a multicast packet sent from the multicast source S, they will all forward the multicast packet to the Ethernet. In this case, the downstream node Router D will receive three copies of the same multicast packet.

In order to avoid such cases, the Assert mechanism is needed to select one forwarder. Routers in the network select the best path through sending Assert packets. If two or more paths have the same priority and metric to the multicast source, the router with the highest IP address will be the upstream neighbor of the (S, G) entry, which is responsible for forwarding the (S, G) multicast packets. The unselected routers will prune the corresponding interfaces to disable the information forwarding.

Introduction to PIM-SM

Protocol independent multicast sparse mode (PIM-SM) is a sparse mode multicast protocol. It is generally used in the following occasions where:

- Group members are sparsely distributed
- The range is wide
- Large scaled networks

In PIM-SM, all hosts do not receive multicast packets by default. Multicast packets are forwarded to the hosts which need multicast packets explicitly.

In order that the receiver can receive the multicast data streams of the specific IGMP group, PIM-SM adopts rendezvous points (RP) to forward multicast information to all PIM-SM routers with receivers. RP is adopted in multicast forwarding. As a result, the network bandwidth that the data packets and control packets occupy is reduced, and the processing overhead of the router is also reduced.

In the receiving end, the router connected to the information receiver sends join messages to the RP corresponding to the multicast group. The join message reaches the root (namely, RP) after passing each router. The passed paths become the branches of the rendezvous point tree (RPT).

If the sending end wants to send data to a multicast group, the first hop router will send registration information to RP. When the registration information reaches RP, the source tree establishing is triggered. Then the multicast source sends the data to RP. When the data reaches RP, the multicast packets are replicated and sent to the receiver. Replication happens only in the branch of RPT. The procedure is repeated automatically until the multicast packets reach the receiver.

PIM-SM is independent of the special unicast routing protocol. Instead, it performs RPF check based on the existing unicast routing table.

Work Mechanism of PIM-SM

The working procedure of PIM-SM is:

- Neighbor discovery
- DR election
- RP discovery
- RPT shared tree building
- Multicast source registration
- Switching RPT to SPT

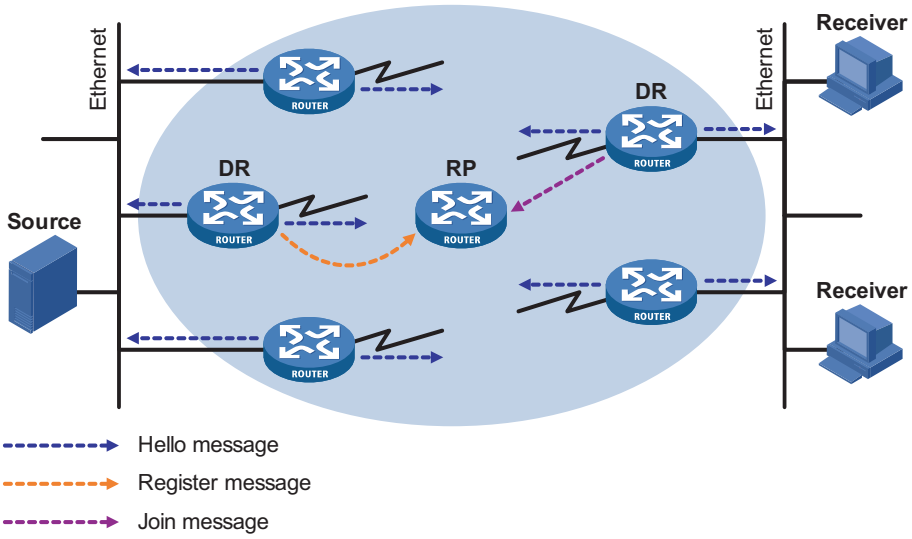
Neighbor discovery

The neighbor discovery mechanism is the same as described in PIM-DM. It is also implemented through Hello messages sent between each router.

DR election

With the help of Hello messages, DR can be elected for the shared network, such as Ethernet. DR will be the unique multicast information forwarder in the network. In either the network connected to the multicast source S or the network connected to the receiver, DR must be elected only if the network is a shared network. The DR in the receiving end sends Join messages to RP and the DR in the multicast source side sends Register messages to RP, as shown in Figure 114:

Figure 114 Diagram for DR election



Each router on the shared network sends Hello messages with the DR priority option to each other. The router with the highest DR priority is elected as the DR in the network. If the priority is the same, the router with the highest IP address is elected as the DR. When DR fails, the received Hello messages will time out. A new DR election procedure will be triggered among neighboring routers.

In PIM-SM network, DR mainly serves as the querier of IGMPv1.

RP discovery

RP is the core router in the PIM-SM domain. The shared tree established based on the multicast routing information is rooted in RP. There is a mapping relationship between the multicast group and RP. One multicast group is mapped to one RP, and multiple multicast groups can be mapped to the same RP.

In a small and simple network, there is only little multicast information. One RP is enough for information forwarding. In this case, you can statically specify the position of RP in each router in the SM domain.

However, PIM-SM network is of very large scale. RP forwards a lot of multicast information. In order to reduce the workload of RP and optimize the topology of the shared tree, different multicast groups must have different RPs. In this case, RP must be elected dynamically through the auto-election mechanism and BootStrap router (BSR) must be configured.

BSR is the core management device in PIM-SM network, which is responsible for:

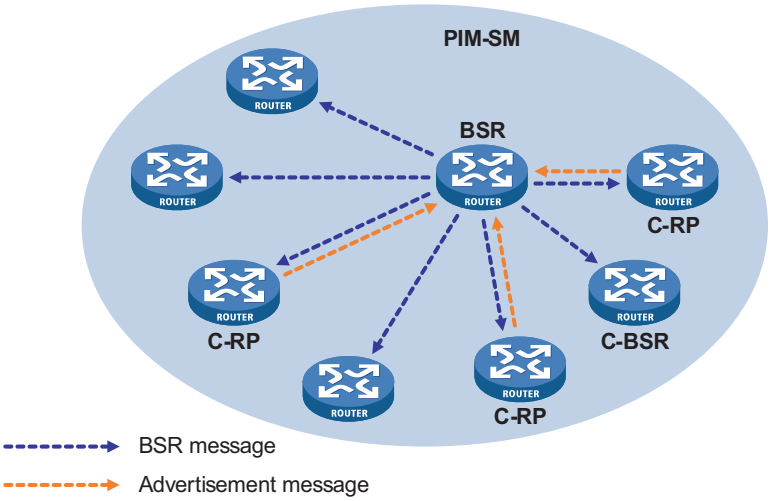
- Collecting the Advertisement messages sent by the Candidate-RP (C-RP) in the network.
- Selecting part of the C-RP information to constitute the RP-set, namely, the mapping database between the multicast group and RP.
- Advertising the RP-set to the whole network in order that all the router (including DR) in the network knows the position of RP.

One or more candidate BSRs must be configured in a PIM domain. Through the auto-election, the candidate BSRs elect a BSR which is responsible for collecting and advertising RP information. The auto-election among candidate BSRs is described in the following section:

- Specify a PIM-SM-enabled interface when configuring a router as a candidate BSR.
- Each candidate BSR considers itself as the BSR of the PIM-SM and uses the IP address of the specified interface as the BSR address to send Bootstrap messages.
- When the candidate BSR receives Bootstrap messages from other routers, it will compare the BSR address in the received Bootstrap message with its own BSR address in priority and IP address. When the priority is the same, the candidate BSR with a higher IP address is considered to be better. If the former is better, the candidate BSR will replace its own BSR address with the new BSR address and does not consider itself as BSR any more. Otherwise, the candidate BSR will keep its own BSR address and continue to consider itself as BSR.

The positions of RPs and BSRs in the network are as shown in Figure 115:

Figure 115 Diagram for the communication between RPs and BSRs



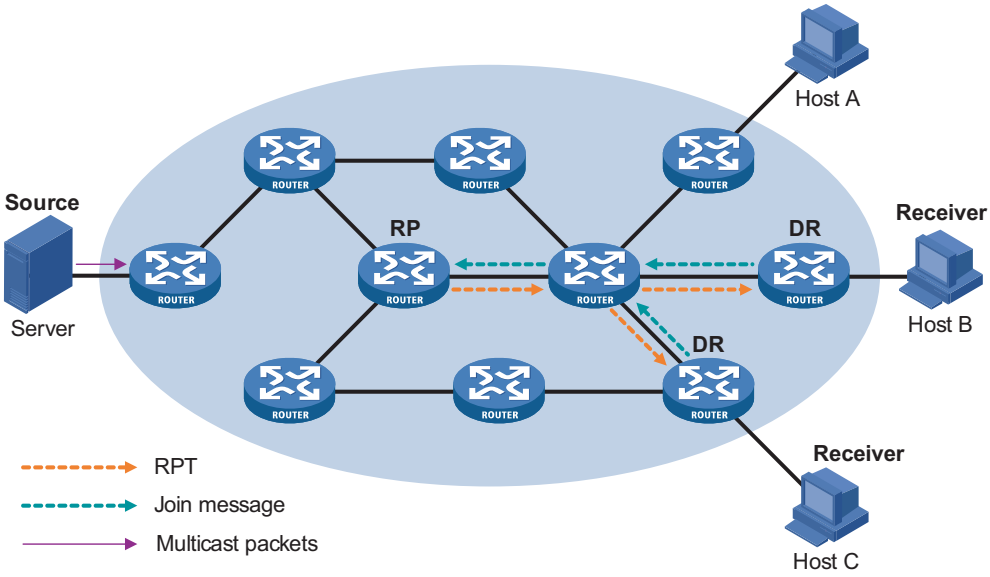
Only one BSR can be elected in a network or management domain, while multiple candidate BSRs (C-BSR) can be configured. In this case, once the BSR fails, other C-BSRs can elect a new BSR through auto-election. Thus, the service is prevented from being interrupted.

In the same way, multiple C-RPs can be configured in a PIM-SM domain, the RP corresponding to each multicast group is worked out through the BSR mechanism.

RPT building

Assume the receiver hosts are User B, User D, and User E. When a receiver host joins in a multicast group G, it will inform the leaf router directly connected to the host through IGMP packets. Thus the leaf router masters the receiver information of the multicast group G, and then the leaf router will send Join messages to the upper-layer nodes in the direction of RP, as shown in Figure 116:

Figure 116 Diagram for RPT building in PIM-SM



Each router on the path from the leaf router to RP will generate (*, G) entries in the forwarding table. The routers on the path forms a branch of RPT. A (*, G) entry represents the information from any source to the multicast group G. RP is the root of RPT and the receivers are leaves of RPT.

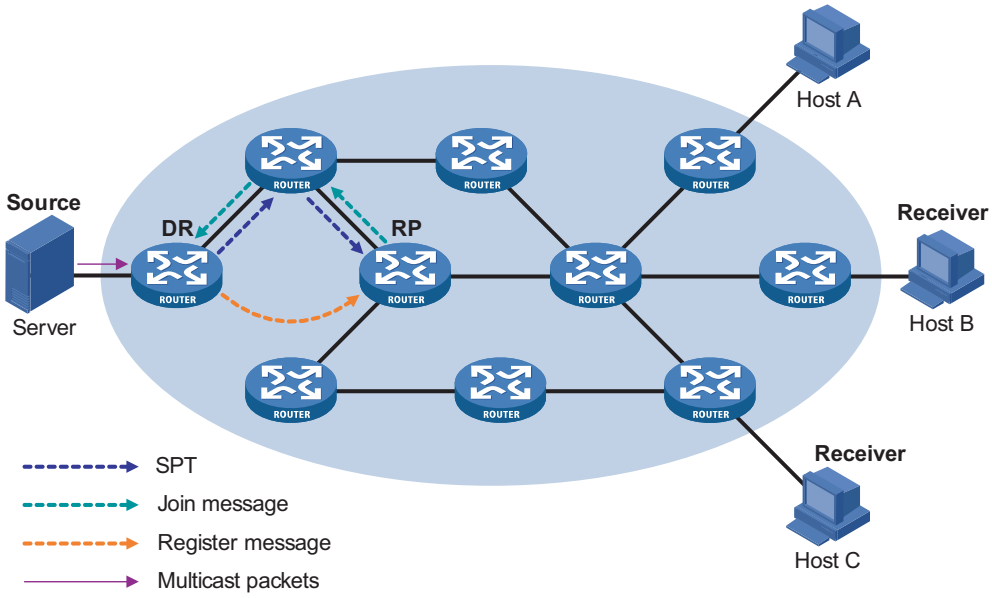
When the packet from the multicast source S to the multicast group G passes by RP, the packet will reach the leaf router and receiver host along the established path in RPT.

When the receiver is not interested in the multicast information any more, the multicast router nearest to the receiver will send Prune messages to RP hop by hop in the direction reverse to RPT. When the first upstream router receives the Prune message, it will delete the links with the downstream routers from the interface list and check whether it has the receivers interested in the multicast information. If not, the upstream router will continue to forward the Prune message to upstream routers.

Multicast source registration

In order to inform RP about the existence of multicast source S, when multicast source S sends a multicast packet to the multicast group G, the router directly connected to S will encapsulate the received packet into a registration packet and send it to the corresponding RP in unicast form, as shown in Figure 117:

Figure 117 Diagram for multicast source registration



When RP receives the registration information from S, it will decapsulate the registration information and forward the multicast information to the receiver along RPT, and on the other hand, it will send (S, G) join messages to S hop by hop. The passed routers constitute a branch of SPT. The multicast source S is the root of SPT and RP is the destination of RP.

The multicast information sent by the multicast source S will reach RP along the built SPT, and then RP will forward the multicast information along the built RPT.

Switching RPT to SPT

When the multicast router nearest to the receiver detects that the rate of the multicast packet from RP to the multicast group G exceeds the threshold value, it will send (S, G) join messages to the upper-layer router of the multicast source S. The join message reaches the router nearest to the multicast source (namely, the first hop router) hop by hop and all the passed routers have the (S, G) entry. As a result, a branch of SPT is built.

Then, the last hop router sends Prune message with the RP bit to RP hop by hop. When RP receives the message, it will reversely forward the Prune message to the multicast source. Thus, the multicast information stream is switched from RPT to SPT.

After the switch from RPT to SPT, the multicast information will be sent from the multicast source S to the receiver directly. Through the switching from RPT to SPT, PIM-SM can build SPT in a more economical way than PIM-DM.

The related threshold values are not set on Switch 7750 Ethernet switches. When the switch receives multicast data forwarded along RPT, it will update the input interface automatically and sends Prune messages to RP.

Common PIM Configuration

You can configure the PIM feature of the switch in interface view. The configuration includes:

Table 372 Configuration tasks

Operation	Description	Related section
Enable PIM-DM (PIM-SM) on the interface	Required	"Enabling PIM-DM (PIM-SM) on the Interface" on page 470
Configure the interval of sending Hello packets	Optional	"Configuring the Interval of Sending Hello Packets" on page 470
Configure PIM neighbors	Optional	"Configuring PIM Neighbors" on page 471
Clear the related PIM entries	Optional	"Clearing the Related PIM Entries" on page 471

Enabling PIM-DM (PIM-SM) on the Interface

Table 373 Enable PIM-DM (PIM-SM) on the interface

Operation	Command	Description
Enter system view	**system-view**	-
Enable the multicast routing protocol	**multicast routing-enable**	Required
Enter VLAN interface view	**interface Vlan-interface** *interface-number*	-
Enable PIM-DM/PIM-SM on the current interface	**pim dm / pim sm**	Optional Configure the PIM protocol type on the interface

Configuring the Interval of Sending Hello Packets

PIM-DM must be enabled on each interface. After the configuration, PIM-DM will send PIM Hello packets periodically and process protocol packets that the PIM neighbors send.

Table 374 Configure the interval of sending Hello packets

Operation	Command	Description
Enter system view	**system-view**	-
Enable the multicast routing protocol	**multicast routing-enable**	Required
Enter VLAN interface view	**interface Vlan-interface** *interface-number*	-
Enable PIM-DM/PIM-SM on the current interface	**pim dm / pim sm**	Required Configure the PIM protocol type on the interface
Configure the interval of sending Hello packets on the interface	**pim timer hello** *seconds*	Required The interval of sending Hello packets is 30 seconds

CAUTION:

- *When PIM-DM is enabled on an interface, PIM-SM cannot be enabled on the interface any more, and vice versa.*
- *When PIM-DM is enabled on an interface of the switch, only PIM-DM can be enabled on the other interfaces of the switch, and vice versa.*

Configuring PIM Neighbors

In order to prevent plenty of PIM neighbors from using out the memory of the router, which may result in router failure, you can limit the number of PIM neighbors on the router interface. However, the total number of PIM neighbors of a router is defined by the system, and you cannot modify it through commands.

You can configure basic ACL 2000 to 2999 (refer to "ACL Configuration" on page 637). Only the filtered Layer 3 switches (routers) cam serve as the PIM neighbors of the current interface.

Table 375 Configure PIM neighbors

Operation	Command	Description
Enter system view	**system-view**	-
Enable the multicast routing protocol	**multicast routing-enable**	Required
Enter VLAN interface view	**interface Vlan-interface** *interface-number*	-
Enable PIM-DM/PIM-SM on the current interface	**pim dm / pim sm**	Required Configure the PIM protocol type on the interface
Configure limit on the number of PIM neighbors on the interface	**pim neighbor-limit** *limit*	Optional By default, the upper limit on the number of PIM neighbors on a interface is 128
Configure the filtering policy for PIM neighbors	**pim neighbor-policy** *acl-number*	Optional ■ You can configure to filter the IP addresses of some multicast groups in ACL. ■ By default, the filtering policy for neighbors cannot be enabled on an interface.



CAUTION: *If the number of existing PIM neighbors exceeds the user-defined limit, the existing PIM neighbors will not be deleted.*

Clearing the Related PIM Entries

You can execute the **reset** command in user view to clear the related statistics about multicast PIM.

Table 376 Clear the related PIM entries

Operation	Command	Description
Clear the PIM route entries	**reset pim routing-table** { **all** | { *group-address* [**mask** *group-mask* | **mask-length** *group-mask-length*] | *source-address* [**mask** *source-mask* | **mask-length** *source-mask-length*] | { **incoming-interface** { *interface-type interface-number* | **null** } } } * }	Perform the configuration in user view.
Clear PIM neighbors	**reset pim neighbor** { **all** | { *neighbor-address* | **interface** *interface-type interface-number* } * }	Perform the configuration in user view.

PIM-DM Configuration

Perform the following configuration to configure PIM-DM. When the router runs in PIM-DM domain, you are recommended to enable PIM-DM on all the interfaces of non-boarder routers.

Configuring Filtering Policies for Multicast Source/Group

Table 377 Configure filtering policies for multicast source/group

Operation	Command	Description
Enter system view	**system-view**	-
Enable the multicast routing protocol	**multicast routing-enable**	Required
Enter PIM view	**pim**	-
Perform source/group filter on the received multicast packets	**source-policy** *acl-number*	Optional You can configure to filter the IP addresses of some multicast groups in ACL.

CAUTION:

- *If you configure basic ACLs, the source address match is performed on all the received multicast packets. The packets failing to match are discarded.*
- *If you configure advanced ACLs, the source address and group address match is performed on all the received multicast packets. The packets failing to match are discarded.*

PIM-SM Configuration

PIM-SM configuration includes:

Table 378 Configuration tasks

Operation	Description	Section
Configure filtering policies for multicast sources/groups	Optional	"Configuring Filtering Policies for Multicast Source/Group" on page 472
Configure BSR/RP	Optional	"Configuring BSR/RP" on page 472
Configure PIM-SM domain boundary	Optional	"Configuring PIM-SM Domain Boundary" on page 474
Filter the registration packets from RP to DR	Optional	"Filtering the Registration Packets from RP to DR" on page 474

Configuring Filtering Policies for Multicast Source/Group

For the configuration of filtering policies for multicast source/group, refer to "PIM-DM Configuration" on page 472.

Configuring BSR/RP

Table 379 Configure BSR/RP

Operation	Command	Description
Enter system view	**system-view**	-
Enable the multicast routing protocol	**multicast routing-enable**	Required
Enter PIM view	**pim**	-

Table 379 Configure BSR/RP

Operation	Command	Description
Configure candidate BSRs	**c-bsr** *interface-type interface-number hash-mask-len* [*priority*]	Optional By default, candidate BSRs are not set for the switch and the value of priority is 0.
Configure candidate RPs	**c-rp** *interface-type interface-number* [**group-policy** *acl-number* | **priority** *priority*]*	Optional ■ You can configure to filter the IP addresses of some multicast groups in ACL. ■ By default, candidate RPs are not set for the switch and the value of priority is 0.
Configure static RPs	**static-rp** *rp-address* [*acl-number*] [**preferred**]	Optional ■ You can configure to filter the IP addresses of some multicast groups in ACL. ■ By default, static RPs are not set for the switch.
Limit the range of valid BSRs	**bsr-policy** *acl-number*	Optional ■ You can configure to filter the IP addresses of some multicast groups in ACL. ■ By default, the range of valid BSRs is not set for the switch.
Limit the range of valid C-RPs	**crp-policy** *acl-number*	Optional ■ You can configure to filter the IP addresses of some multicast groups in ACL. ■ By default, the range of valid C-RPs is not set for the switch.



CAUTION:

- *Only one candidate BSR can be configured on a Layer 3 switch. The BSR configuration on another interface will replace the former configuration.*
- *You are recommended to configure both the candidate BSR and candidate RP on the Layer 3 switch in the backbone.*
- *If the range of multicast groups that RP serves is not specified when RP is configured, the RP serves all multicast groups. Otherwise, the RP serves the multicast groups within the specified range.*
- *You can configure basic ACLs to filter related multicast IP addresses and control the range of multicast groups that RP serves.*
- *If you use static RPs, all routers in the PIM domain must adopt the same configuration.*
- *If the configured static RP address is the address of an UP interface on the local switch, the switch will serve as RP.*

- *If both a dynamic RP and a static RP exist simultaneously, and if you have configured the keyword **preferred**, the static RP has the priority over the dynamic RP.*
- *The PIM protocol need not be enabled on the interface of static RPs.*
- *The limit on the range of valid BSRs is to prevent the valid BSRs in the network being replaced maliciously. The other BSR information except the range will not be received by the Layer 3 switch, and thus the security of BSRs in the network is protected.*
- *The limit on the range of C-RPs is to avoid C-RP cheating. You can limit the range of valid C-RPs and limit the range of multicast groups that each C-RP serves.*

Configuring PIM-SM Domain Boundary

Table 380 Configure PIM-SM domain boundary

Operation	Command	Description
Enter system view	**system-view**	-
Enable the multicast routing protocol	**multicast routing-enable**	Required
Enter VLAN interface view	**interface Vlan-interface** *interface-number*	-
Enable PIM-SM on the current interface	**pim sm**	Required Configure the PIM protocol type on the interface.
Configure PIM-SM domain boundary	**pim bsr-boundary**	Required By default, domain boundary is not set for the switch.



CAUTION:

- *When the PIM-SM domain boundary is set, Bootstrap messages cannot pass the boundary in any direction. In this way, PIM-SM domains are divided.*
- *When this feature is configured, Bootstrap messages cannot pass the boundary. However, the other PIM messages can pass the domain boundary. The network can be effectively divided into domains using different BSRs.*

Filtering the Registration Packets from RP to DR

Through the registration packet filtering mechanism in PIM-SM network, you can determine which sources send packets to which groups on RP, that is, RP can filter the registration packets from DR and receive the specified packets only.

Table 381 Filter the registration packets from RP to DR

Operation	Command	Description
Enter system view	**system-view**	-
Enable the multicast routing protocol	**multicast routing-enable**	Enable the multicast routing protocol
Enter VLAN interface view	**interface Vlan-interface** *interface-number*	-
Enable IGMP on the current interface	**pim sm**	Required Configure the PIM protocol type on the interface

Table 381 Filter the registration packets from RP to DR

Operation	Command	Description
Quit VLAN view	**quit**	-
Enter PIM view	**pim**	-
Configure to filter the registration packets from RP to DR	**register-policy** *acl-number*	Required ■ You can configure to filter the IP addresses of some multicast groups in ACL. ■ By default, the switch does not filter the registration packets from DR.

CAUTION:

- *If a source group entry (S, G) is denied in ACL, or no operation on the entry is defined in the ACL, or ACLs are not defined, RP will send RegisterStop messages to DR to stop the registration process of the multicast data flow.*
- *Only the registration packets matching the **permit** command of ACLs can be accepted When an invalid ACL is defined, RP will reject all the registration packets.*

Configuring the Threshold for RPT-to-SPT Switchover

Initially, a PIM-SM router forwards multicast packets through an RPT. However, when the traffic rate of multicast packets reaches a configurable threshold, the last-hop router that these multicast packets pass will initiate an RPT-to-SPT switchover.

Table 382 Set the threshold for RPT-to-SPT switchover

Operation	Command	Description
Enter system view	**system-view**	-
Enter PIM view	**pim**	Required
Set the threshold for RPT-to-SPT switchover	**spt-switch-threshold** { traffic-rate | **infinity** } [**group-policy** acl-number [**order** *order-value*]]	Optional The threshold is 0 by default.

*Only the threshold 0 and the **infinity** keyword are supported currently.*

- *If the threshold is set to 0, the last-hop switch performs RPT-to-SPT switchover upon receiving the first multicast packet.*
- *The **infinity** keyword specifies that RPT-to-SPT switchover never takes place.*

Displaying and Debugging PIM

After completing the above configurations, you can execute the **display** command in any view to verify the configuration by checking the displayed information.

Table 383 Display and maintain PIM

Configuration	Command	Description
Display PIM multicast routing tables	**display pim routing-table** [{ { ***g** [*group-address* [**mask** { *mask-length* | *mask* }]] | ****rp** [*rp-address* [**mask** { *mask-length* | *mask* }]] } | { *group-address* [**mask** { *mask-length* | *mask* }] | *source-address* [**mask** { *mask-length* | *mask* }] } ***** } | **incoming-interface** { *interfac e-type interface-number* | **null** } | { **dense-mode** | **sparse-mode** }] *****	You can execute the **display** command in any view.
Display the information about PIM interfaces	**display pim interface** [*interface-type interface-number*]	
Display the information about PIM neighbor routers	**display pim neighbor** [**interface** *interface-type interface-number*]	
Display BSR information	**display pim bsr-info**	
Display RP information	**display pim rp-info** [*group-address*]	

PIM Configuration Examples

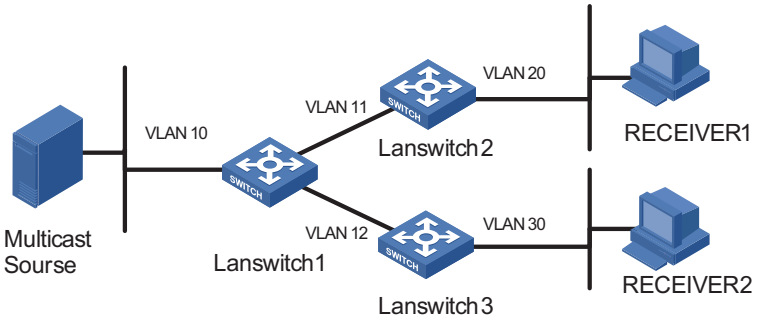
PIM-DM Configuration Example

Network requirements

Lanswitch 1 is connected to Multicast Source through Vlan-interface 10, to Lanswitch 2 through Vlan-interface 11 and to Lanswitch3 through Vlan-interface 12. Through PIM-DM, multicast is implemented among Receiver 1, Receiver 2 and Multicast Source.

Network diagram

Figure 118 Network diagram for PIM-DM configuration



Configuration procedure

1 Configure unicast routing

Configure the OSPF protocol for interoperation among the switches in the PIM-DM domain. Ensure the network-layer interoperation among the switches in the PIM-DM domain. Detailed configuration steps are omitted here.

2 Enable IP multicast routing, and enable PIM-DM on each interface

Enable multicast routing on Lanswitch 1, and enable PIM-DM on each interface.

```
<Lanswitch1> system-view
[Lanswitch1] multicast routing-enable
[Lanswitch1] interface Vlan-interface 10
[Lanswitch1-Vlan-interface10] pim dm
[Lanswitch1-Vlan-interface10] quit
[Lanswitch1] interface Vlan-interface 11
[Lanswitch1-Vlan-interface11] pim dm
[Lanswitch1-Vlan-interface11] quit
[Lanswitch1] interface Vlan-interface 12
[Lanswitch1-Vlan-interface12] pim dm
```

Enable multicast routing on Lanswitch 2, enable PIM-DM on each interface, and enable IGMP on Vlan-interface 20.

```
<Lanswitch2> system-view
[Lanswitch2] multicast routing-enable
[Lanswitch2] interface Vlan-interface 11
[Lanswitch2-Vlan-interface11] pim dm
[Lanswitch2-Vlan-interface11] quit
[Lanswitch2] interface Vlan-interface 20
[Lanswitch2-Vlan-interface12] pim dm
[Lanswitch2-Vlan-interface12] igmp enable
```

The configuration on Lanswitch 3 is similar to the configuration on Lanswitch 2.

PIM-SM Configuration Example

Network requirements

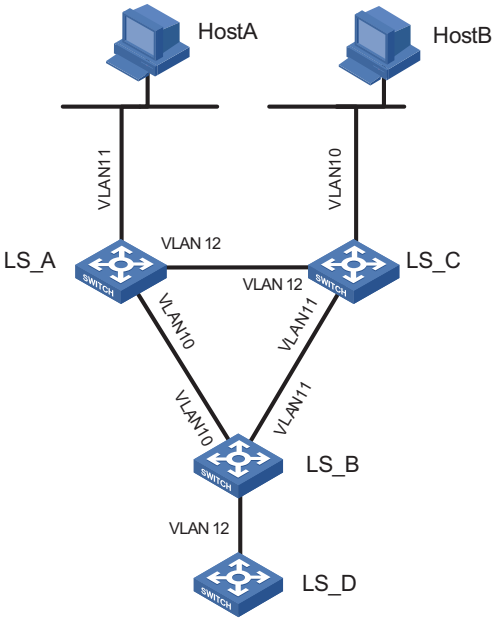
All Ethernet switches are reachable for each other in the practical network.

- LS_A is connected to LS_B through Vlan-interface 10, to Host A through Vlan-interface 11 and to LS_C through Vlan-interface 12.
- LS_B is connected to LS_A through Vlan-interface 10, to LS_C through Vlan-interface 11 and to LS_D through Vlan-interface 12.
- LS_C is connected to Host B through Vlan-interface 10, to LS_B through Vlan-interface 11 and to LS_A through Vlan-interface 12.

Host A is the receiver of the multicast group whose multicast IP address is 225.0.0.1. Host B begins to send data to the destination 225.0.0.1 and LS_A receives the multicast data from Host B through LS_B.

Network diagram

Figure 119 Network diagram for PIM-SM configuration



Configuration procedure

1 Configure unicast routing

Configure the OSPF protocol for interoperation among the switches in the PIM-SM domain. Ensure the network-layer interoperation among the switches in the PIM-SM domain. Detailed configuration steps are omitted here.

2 Enable IP multicast routing, and enable PIM-SM on each interface

- Configure LS_A

Enable multicast routing, enable PIM-SM on each interface, and enable IGMP on Vlan-interface 11.

```
<SW7750> system-view
[SW7750] multicast routing-enable
[SW7750] interface Vlan-interface 10
[SW7750-Vlan-interface10] pim sm
[SW7750-Vlan-interface10] quit
[SW7750] interface Vlan-interface 11
[SW7750-Vlan-interface11] pim sm
[SW7750-Vlan-interface11] igmp enable
[SW7750-Vlan-interface11] quit
[SW7750] interface Vlan-interface 12
[SW7750-Vlan-interface12] pim sm
```

- Configure LS_B

Enable multicast routing, and enable PIM-SM on each interface.

```
<SW7750> system-view
[SW7750] multicast routing-enable
[SW7750] interface Vlan-interface 10
```

```
[SW7750-Vlan-interface10] pim sm
[SW7750-Vlan-interface10] quit
[SW7750] interface Vlan-interface 11
[SW7750-Vlan-interface11] pim sm
[SW7750-Vlan-interface11] quit
[SW7750] interface Vlan-interface 12
[SW7750-Vlan-interface12] pim sm
[SW7750-Vlan-interface12] quit
```

Configure candidate BSRs.

```
[SW7750] pim
[SW7750-pim] c-bsr Vlan-interface 10 30
```

Configure candidate RPs.

```
[SW7750] acl number 2000
[SW7750-acl-basic-2000] rule permit source 225.0.0.0 0.255.255.255
[SW7750] pim
[SW7750-pim] c-rp Vlan-interface 10 group-policy 2000
```

Configure a PIM domain boundary.

```
[SW7750] interface Vlan-interface 12
[SW7750-Vlan-interface12] pim bsr-boundary
```

When Vlan-interface 12 is configured as the PIM domain boundary, LS_D cannot receive BSR information from LS_B any mote, that is, LS_D is excluded from the PIM domain.

- Configure LS_C

The configuration on LS_C is similar to the configuration on LS_A.

Troubleshooting PIM

Symptom 1: The router cannot set up multicast routing tables correctly.

Solution: You can troubleshoot PIM according to the following procedure.

Make sure that the unicast routing is right before troubleshooting PIM.

- Because PIM-SM needs the support of RP and BSR, you must execute the display pim bsr-info command to see whether BSR information exists. If not, you must check whether there are unicast routes to the BSR. Then use the display pim rp-info command to check whether the RP information is right. If RP information does not exist, you must check whether there are unicast routes to RP.
- Use the display pim neighbor command to check whether the neighboring relationship is correctly established.

48 MSDP CONFIGURATION

MSDP Overview

Introduction to MSDP

Multicast Source Discovery Protocol (MSDP) is an inter-domain multicast solution developed to address the interconnection of Protocol Independent Multicast sparse mode (PIM-SM) domains. It is used to discover multicast source information in other PIM-SM domains.

In the basic PIM-SM mode, a multicast source registers only with the RP in the local PIM-SM domain, and the multicast source information of a domain is isolated from that of another domain. As a result, the RP is aware of the source information only within the local domain and a multicast distribution tree is built only within the local domain to deliver multicast data from a local multicast source to local receivers. If there is a mechanism that allows RPs of different PIM-SM domains to share their multicast source information, the local RP will be able to join multicast sources in other domains and multicast data can be transmitted among different domains.

MSDP achieves this objective. By establishing MSDP peer relationships among RPs of different PIM-SM domains, source active (SA) messages can be forwarded among domains and the multicast source information can be shared.



CAUTION:

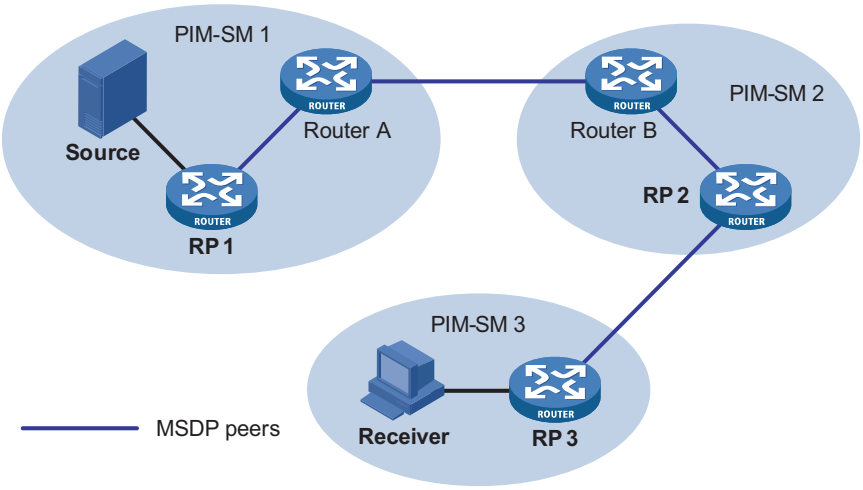
- *MSDP is applicable only if the intra-domain multicast protocol is PIM-SM.*
- *MSDP is meaningful only for the any-source multicast (ASM) model.*

How MSDP Works

MSDP peers

With one or more pairs of MSDP peers configured in the network, an MSDP interconnection map is formed, where the RPs of different PIM-SM domains are interconnected in series. Relayed by these MSDP peers, an SA message sent by an RP can be delivered to all other RPs.

Figure 120 Where MSDP peers are in the network



As shown in Figure 120, an MSDP peer can be created on any PIM-SM router. MSDP peers created on PIM-SM routers that assume different roles function differently.

1 MSDP peers on RPs

- Source-side MSDP peer: the MSDP peer nearest to the multicast source (Source), typically the source-side RP, like RP 1. The source-side RP creates SA messages and sends the messages to its remote MSDP peer to notify the MSDP peer of the locally registered multicast source information. A source-side MSDP must be created on the source-side RP; otherwise it will not be able to advertise the multicast source information out of the PIM-SM domain.
- Receiver-side MSDP peer: the MSDP peer nearest to the receivers, typically the receiver-side RP, like RP 3. Upon receiving an SA message, the receiver-side MSDP peer resolves the multicast source information carried in the message and joins the SPT rooted at the source across the PIM-SM domain. When multicast data from the multicast source arrives, the receiver-side MSDP peer forwards the data to the receivers along the RPT.
- Intermediate MSDP peer: an MSDP peer with multicast remote MSDP peers, like RP 2. An intermediate MSDP peer forwards SA messages received from one remote MSDP peer to other remote MSDP peers, functioning as a relay of multicast source information.

2 MSDP peers created on common PIM-SM routers (other than RPs)

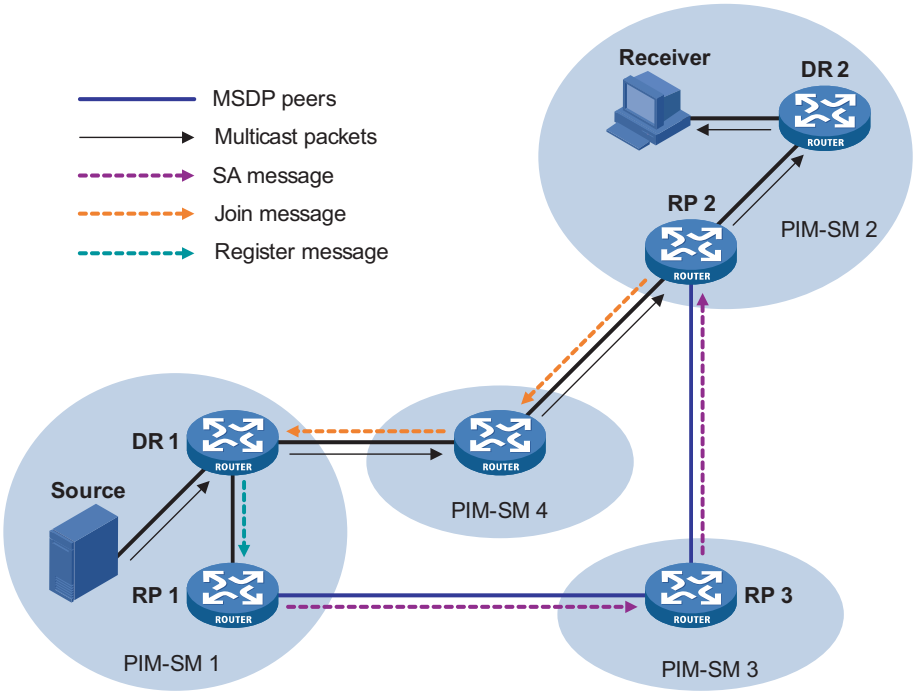
Router A and Router B are MSDP peers on common multicast routers. Such MSDP peers just forward received SA messages.

An RP is dynamically elected from C-RPs. To enhance network robustness, a PIM-SM network typically has more than one C-RP. As the RP election result is unpredictable, MSDP peering relationships should be built among all C-RPs so that the winner C-RP is always on the "MSDP interconnection map", while loser C-RPs will assume the role of common PIM-SM routers on the "MSDP interconnection map".

Implementing inter-domain multicast delivery by leveraging MSDP peers

As shown in Figure 121, an active source (Source) exists in the domain PIM-SM 1, and RP 1 has learned the existence of Source through multicast source registration. If RPs in PIM-SM 2 and PIM-SM 3 also wish to know the specific location of Source so that receiver hosts can receive multicast traffic originated from it, MSDP peering relationships should be established between RP 1 and RP 3 and between RP 3 and RP 2 respectively.

Figure 121 MSDP peering relationships



The process if implementing inter-domain multicast delivery by leveraging MSDP peers is as follows:

1. When the multicast source in PIM-SM 1 sends the first multicast packet to multicast group G, DR 1 encapsulates the multicast data within a register message and sends the register message to RP 1. Then, RP 1 gets aware of the information related to the multicast source.
2. As the source-side RP, RP 1 creates SA messages and periodically sends the SA messages to its MSDP peer. An SA message contains the source address (S), the multicast group address (G), and the address of the RP which has created this SA message (namely RP 1).
3. On MSDP peers, each SA message is subject to a Reverse Path Forwarding (RPF) check and multicast policy-based filtering, so that only SA messages that have arrived along the correct path and passed the filtering are received and forwarded. This avoids delivery loops of SA messages. In addition, you can configure MSDP peers into an MSDP mesh group so as to avoid flooding of SA messages between MSDP peers.
4. SA messages are forwarded from one MSDP peer to another, and finally the information of the multicast source traverses all PIM-SM domains with MSDP peers (PIM-SM 2 and PIM-SM 3 in this example).

5 Upon receiving the SA message created by RP 1, RP 2 in PIM-SM 2 checks whether there are any receivers for the multicast group in the domain.

- If so, the RPT for the multicast group G is maintained between RP 2 and the receivers. RP 2 creates an (S, G) entry, and sends an (S, G) join message hop by hop towards DR 1 at the multicast source side, so that it can directly join the SPT rooted at the source over other PIM-SM domains. Then, the multicast data can flow along the SPT to RP 2 and is forwarded by RP 2 to the receivers along the RPT. Upon receiving the multicast traffic, the DR at the receiver side (DR 2) decides whether to initiate an RPT-to-SPT switchover process.
- If no receivers for the group exist in the domain, RP 2 does dot create an (S, G) entry and does not join the SPT rooted at the source.

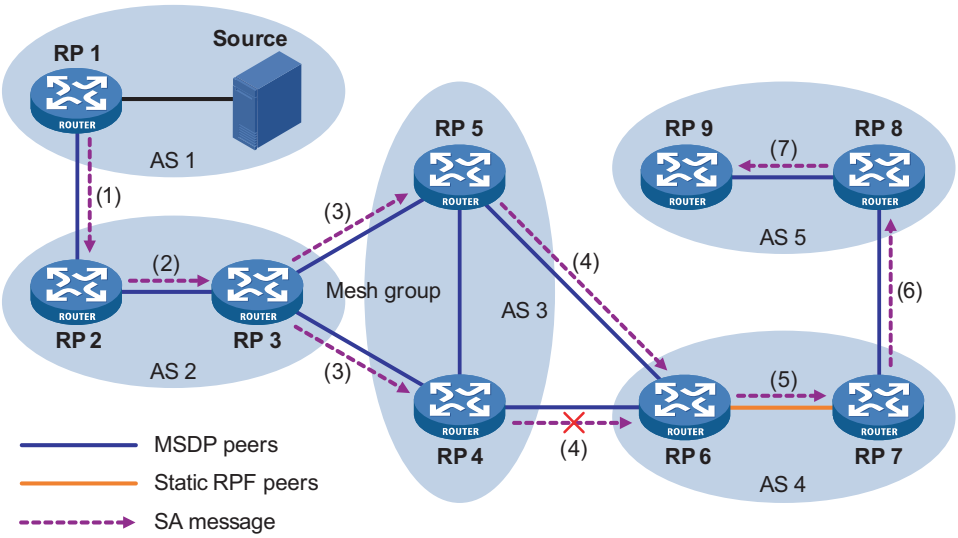
- *An MSDP mesh group refers to a group of MSDP peers that have MSDP peering relationships among one another and share the same group name.*
- *When using MSDP for inter-domain multicasting, once an RP receives information from a multicast source, it no longer relies on RPs in other PIM-SM domains. The receivers can override the RPs in other domains and directly join the multicast source-based SPT.*

RPF check rules for SA messages

As shown in Figure 122, there are five autonomous systems in the network, AS 1 through AS 5, with IGP enabled on routers within each AS and EBGP as the interoperation protocol among different ASs. Each AS contains at least one PIM-SM domain and each PIM-SM domain contains one or more RPs. MSDP peering relationships have been established among different RPs. RP 3, RP 4 and RP 5 are in an MSDP mesh group. On RP 7, RP 6 is configured as its static RPF peer.

If only one MSDP peer exists in a PIM-SM domain, this PIM-SM domain is also called a stub domain. For example, AS 4 in Figure 122 is a stub domain. The MSDP peer in a stub domain can have multiple remote MSDP peers at the same time. You can configure one or more remote MSDP peers as static RPF peers. When an RP receives an SA message from a static RPF peer, the RP accepts the SA message and forwards it to other peers without performing an RPF check.

Figure 122 Diagram for RPF check for SA messages



As illustrated in Figure 122, these MSDP peers dispose of SA messages according to the following RPF check rules:

1 When RP 2 receives an SA message from RP 1

Because the source-side RP address carried in the SA message is the same as the MSDP peer address, which means that the MSDP peer where the SA is from is the RP that has created the SA message, RP 2 accepts the SA message and forwards it to its other MSDP peer (RP 3).

2 When RP 3 receives the SA message from RP 2

Because the SA message is from an MSDP peer (RP 2) in the same AS, and the MSDP peer is the next hop on the optimal path to the source-side RP, RP 3 accepts the message and forwards it to other peers (RP 4 and RP 5).

3 When RP 4 and RP 5 receive the SA message from RP 3

Because the SA message is from an MSDP peer (RP 3) in the same mesh group, RP 4 and RP 5 both accept the SA message, but they do not forward the message to other members in the mesh group; instead, they forward it to other MSDP peers (RP 6 in this example) out of the mesh group.

4 When RP 6 receives the SA messages from RP 4 and RP 5 (suppose RP 5 has a higher IP address)

Although RP 4 and RP 5 are in the same SA (AS 3) and both are MSDP peers of RP 6, because RP 5 has a higher IP address, RP 6 accepts only the SA message from RP 5.

5 When RP 7 receives the SA message from RP 6

Because the SA message is from a static RPF peer (RP 6), RP 7 accepts the SA message and forwards it to other peer (RP 8).

6 When RP 8 receives the SA message from RP 7

An EBGP route exists between two MSDP peers in different ASs. Because the SA message is from an MSDP peer (RP 7) in a different AS, and the MSDP peer is the next hop on the EBGP route to the source-side RP, RP 8 accepts the message and forwards it to its other peer (RP 9).

7 When RP 9 receives the SA message from RP 8

Because RP 9 has only one MSDP peer, RP 9 accepts the SA message.

SA messages from other paths than described above will not be accepted nor forwarded by MSDP peers.

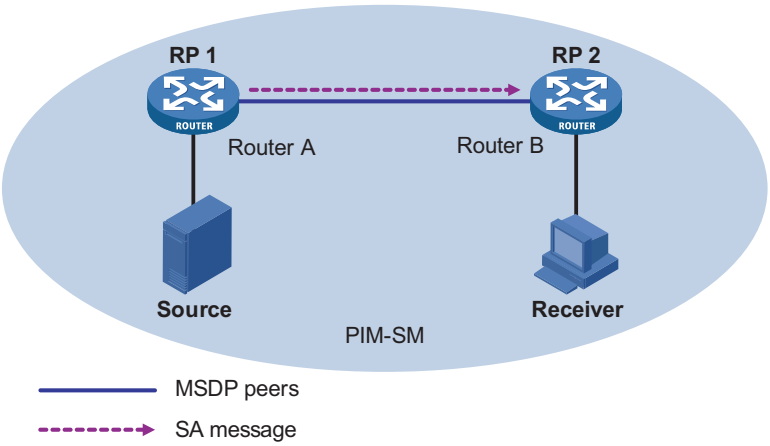
Implementing intra-domain Anycast RP by leveraging MSDP peers

Anycast RP refers to such an application that enables load balancing and redundancy backup between two or more RPs within a PIM-SM domain by configuring the same IP address for, and establishing MSDP peering relationships between, these RPs.

As shown in Figure 123, within a PIM-SM domain, a multicast source sends multicast data to multicast group G, and Receiver is a member of the multicast group. To implement Anycast RP, configure the same IP address (known as anycast RP address, typically a private address) on Router A and Router B, configure these interfaces as C-RPs, and establish an MSDP peering relationship between Router A and Router B.

Usually an Anycast RP address is configured on a logic interface, like a loopback interface.

Figure 123 Typical network diagram of Anycast RP



The work process of Anycast RP is as follows:

1. The multicast source registers with the nearest RP. In this example, Source registers with RP 1, with its multicast data encapsulated in the register message. When the register message arrives at RP 1, RP 1 decapsulates the message.
2. Receivers send join messages to the nearest RP to join the RPT rooted as this RP. In this example, Receiver joins the RPT rooted at RP 2.
3. RPs share the registered multicast information by means of SA messages. In this example, RP 1 creates an SA message and sends it to RP 2, with the multicast data from Source encapsulated in the SA message. When the SA message reaches RP 2, RP 2 decapsulates the message.
4. Receivers receive the multicast data along the RPT and directly join the SPT rooted at the multicast source. In this example, RP 2 forwards the multicast data down the RPT. When Receiver receives the multicast data from Source, it directly joins the SPT rooted at Source.

The significance of Anycast RP is as follows:

- Optimal RP path: A multicast source registers with the nearest RP so that an SPT with the optimal path is built; a receiver joins the nearest RP so that an RPT with the optimal path is built.
- Load balancing between RPs: Each RP just needs to maintain part of the source/group information within the PIM-SM domain and forward part of the multicast data, thus achieving load balancing between different RPs.

- Redundancy backup between RPs: When an RP fails, the multicast source previously registered with it or the receivers previous joined it will register with or join another nearest RP, thus achieving redundancy backup between RPs.

CAUTION:

- *Be sure to configure a 32-bit subnet mask (255.255.255.255) for the Anycast RP address, namely configure the Anycast RP address into a host address.*
- *An MSDP peer address must be different from the Anycast RP address.*

Protocols and Standards

MSDP is documented in the following specifications:

- RFC 3618: Multicast Source Discovery Protocol (MSDP)
- RFC 3446: Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)

Configuring MSDP Basic Functions

To enable exchange of information from the multicast source S between two PIM-SM domains, you need to establish MSDP peering relationships between RPs in these PIM-SM domains. In this way, the information from the multicast source can be sent through SA messages between the MSDP peers, and the receivers in other PIM-SM domains can finally receive the multicast source information.

A BGP or MBGP route is required between two routers that are MSDP peers to each other. Through this route, the two routers can transfer SA messages between PIM-SM domains, so BGP peers are the basic for establishing MSDP peers.

For an area containing only one MSDP peer, known as a stub area, the BGP or MBGP route is not compulsory. SA messages are transferred in a stub area through the static RPF peers. In addition, the use of static RPF peers can avoid RPF check on the received SA messages, thus saving resources.

Before configuring static RPF peers, you must create an MSDP peering connection. If you configure only one MSDP peer on a router, the MSDP peer will act as a static RPF peer. If you configure multiple static RPF peers, you need to handle them by using different rules according to whether the **rp-policy** keyword is used to configure the filtering policies.

When configuring multiple static RPF peers for the same router, you must follow the following two configuration methods:

- In the case that all the peers use the **rp-policy** keyword: Multiple static RPF peers function at the same time. RPs in SA messages are filtered based on the configured prefix list, and only the SA messages whose RP addresses pass the filtering are received. If multiple static RPF peers using the same **rp-policy** keyword are configured, when any of the peers receives an SA message, it will forward the SA message to other peers.
- None of the peers use the **rp-policy** keyword: Based on the configured sequence, only the first static RPF peer whose connection state is UP is active. All the SA messages from this peer will be received, while the SA messages from other static RPF peers will be discarded. Once the active static RPF peer fails (because the configuration is removed or the connection is terminated), based on the configuration sequence, the subsequent first static RPF peer

whose connection is in the UP state will be selected as the active static RPF peer.

Configuration Prerequisites

Before configuring basic MSDP functions, you need to configure:

- A unicast routing protocol
- Basic functions of PIM-SM
- Basic functions of BGP

Configuring MSDP Basic Functions

Table 384 Configure MSDP basic functions

Operation	Command	Description
Enter system view	**system-view**	-
Enable IP multicast routing	**multicast routing-enable**	Required Other multicast configurations do not take effect until multicast routing is enabled.
Enable MSDP function and enter MSDP view	**msdp**	Required Enable MSDP
Create an MSDP peer connection	**peer** *peer-address* **connect-interface** *interface-type interface-number*	Required To establish an MSDP peer connection, you must configure the parameters on both peers. The peers are identified by an address pair (the address of the interface on the local router and the IP address of the remote MSDP peer).
Configure a static RPF peer	**static-rpf-peer** *peer-address* [**rp-policy** *ip-prefix-name*]	Optional For an area containing only one MSDP peer, if BGP or MBGP does not run in this area, you need to configure a static RPF peer.



- *Enable BGP or MBGP on a MSDP-enabled router. You are recommended to assign the same address for a BGP peer or MBGP peer as the MSDP peer on a router.*
- *If a router interface serves as one end of a MSDP peer and BGP peer simultaneously, you need to configure the same IP address for both the MSDP peer and the BGP peer.*

Configuring Connection between MSDP Peers

An AS may contain multiple MSDP peers. To avoid SA flooding between the MSDP peers, you can use the MSDP mesh mechanism to improve traffic. When multiple MSDP peers are fully connected with one another, these MSDP peers form a mesh group. When an MSDP peer in the mesh group receives SA messages from outside the mesh group, it sends them to other members of the group. On the other hand, a mesh group member does not perform RPF check on SA messages from within the mesh group and does not forward the messages to other members of the mesh group. This avoids SA message flooding since it is unnecessary to run

BGP or MBGP between MSDP peers, thus simplifying the RPF checking mechanism.

The sessions between MSDP peers can be terminated and reactivated sessions as required. When a session between MSDP peers is terminated, the TCP connection is closed, and there will be no reconnection attempts. However, the configuration information is kept.

Configuration Prerequisites

Before configuring an MSDP peer connection, you need to configure:

- A unicast routing protocol
- Basic functions of IP multicast
- PIM-SM basic functions
- MSDP basic functions

Configuring Description Information for MSDP Peers

You can configure description information for each MSDP peer to manage and memorize the MSDP peers.

Table 385 Configure description information for an MSDP peer

Operation	Command	Description
Enter system view	**system-view**	-
Enter MSDP view	**msdp**	-
Configure description information for an MSDP peer	**peer** *peer-address* **description** *text*	Optional By default, an MSDP peer has no description text.

Configuring Anycast RP Application

If you configure RPs with the same address for two routers in the same PIM-SM domain, the two routers will be MSDP peers to each other. To prevent failure of RPF check on SA messages between MSDP peers, you must configure the RP address to be carried in the SA messages.

Table 386 Configure anycast RP application

Operation	Command	Description
Enter system view	**system-view**	-
Enter MSDP view	**msdp**	-
Create an MSDP peer connection	**peer** *peer-address* **connect-interface** *interface-type interface-number*	Required
Configure the RP address to be carried in SA messages	**originating-rp** *interface-type interface-number*	Required



In Anycast RP application, C-BSR and C-RP must be configured on different devices or ports.

Configuring an MSDP Mesh Group

Configure a mesh group name on all the peers that will become members of the MSDP mesh group so that the peers are fully connected with one another in the mesh group.

Table 387 Configure an MSDP mesh group

Operation	Command	Description
Enter system view	**system-view**	-
Enter MSDP view	**msdp**	-
Add an MSDP peer to a mesh group	**peer** *peer-address* **mesh-group** *name*	Required This command must be configured on all the peers; therefore, you need to configure this command for multiple times.



- *Before you configure an MSDP mesh group, make sure that the routers are fully connected with one another.*
- *The same group name must be configured on all the peers.*
- *If you add the same MSDP peer to multiple mesh groups, only the latest configuration takes effect.*

Configuring MSDP Peer Connection Control

The connection between MSDP peers can be flexibly controlled. You can disable the MSDP peering relationships temporarily by shutting down the MSDP peers. As a result, SA messages cannot be transmitted between these two peers. On the other hand, when resetting an MSDP peering relationship between faulty MSDP peers or bringing faulty MSDP peers back to work, you can adjust the retry interval of establishing a peering relationship through the following configuration.

Table 388 Configure MSDP peer connection control

Operation	Command	Description
Enter system view	**system-view**	-
Enter MSDP view	**msdp**	-
Shut down an MSDP peer	**shutdown** *peer-address*	Optional
Configure retry interval of setting up an MSDP peer connection	**timer retry** *seconds*	Optional The default value is 30 seconds.

Configuring SA Message Transmission

An SA message contains the IP address of the multicast source S, multicast group address G, and RP address. In addition, it contains the first multicast data received by the RP in the domain where the multicast source resides. For some burst multicast data, if the multicast data interval exceeds the SA message hold time, the multicast data must be encapsulated in the SA message; otherwise, the receiver will never receive the multicast source information.

By default, when a new receiver joins, a router does not send any SA request message to its MSDP peer but has to wait for the next SA message. This defers the reception of the multicast information by the receiver. In order for the new receiver to know about the currently active multicast source as quickly as possible, the router needs to send SA request messages to the MSDP peer.

Generally, a router accepts all SA messages sent by all MSDP peers and sends all SA messages to all MSDP peers. By configuring the rules for filtering SA messages to receive/send, you can effectively control the transmission of SA messages

among MSDP peers. For forwarded SA messages, you can also configure a Time-to-Live (TTL) threshold to control the range where SA messages carrying encapsulated data are transmitted.

To reduce the delay in obtaining the multicast source information, you can cache SA messages on the router. The number of SA messages cached must not exceed the system limit. The more messages are cached, the more router memory is occupied. You need to determine the number of cached SA messages as required.

Configuration Prerequisites

Before you configure SA message transmission, perform the following tasks:

- Configuring a unicast routing protocol.
- Configuring basic IP multicast functions.
- Configuring basic PIM-SM functions.
- Configuring basic MSDP functions.

Configuring the Transmission and Filtering of SA Request Messages

After you configure to request SA messages from MSDP peers, when a router receives a Join message, it sends an SA request message to the specified remote MSDP peer, which responds with an SA message that it has cached. After sending an SA request message, the router will get immediately a response from all active multicast sources. By default, the router does not send any SA request message to its MSDP peers upon receipt of a Join message; instead, it waits for the next SA message.

The SA message that the remote MSDP peer responds with is cached in advance; therefore, you must enable the SA message caching mechanism in advance. Typically, only the routers caching SA messages can respond to SA request messages.

After you have configured a rule for filtering received SA messages, if no ACL is specified, all SA request messages sent by the corresponding MSDP peer will be ignored; if an ACL is specified, the SA request messages that satisfy the ACL rule are received while others are ignored.

Table 389 Configure the transmission and filtering of SA request messages

Operation	Command	Description
Enter system view	**system-view**	-
Enter MSDP view	**msdp**	-
Enable SA message caching mechanism	**cache-sa-enable**	Optional By default, the router caches the SA state upon receipt of an SA message.
Configure to request SA messages from an MSDP peer	**peer** *peer-address* **request-sa-enable**	Optional By default, upon receipt of a Join message, the router sends no SA request message to its MSDP peer but waits for the next SA message.

Table 389 Configure the transmission and filtering of SA request messages

Operation	Command	Description
Configure to filter the SA messages received by an MSDP peer	**peer** *peer-address* **sa-request-policy** [**acl** *acl-number*]	Optional By default, a router receives all SA request messages from the MSDP peer.

Configuring a Rule for Filtering the Multicast Sources of SA Messages

An RP filters each registered source to control the information of active sources advertised in the SA message. An MSDP peer can be configured to advertise only the (S, G) entries in the multicast routing table that satisfy the filtering rule when the MSDP creates the SA message; that is, to control the (S, G) entries to be imported from the multicast routing table to the PIM-SM domain. If the **import-source** command is executed without the **acl** keyword, no source will be advertised in the SA message.

Table 390 Configure a rule for filtering multicast sources using SA messages

Operation	Command	Description
Enter system view	**system-view**	-
Enter MSDP view	**msdp**	-
Configure to filter multicast sources using SA messages	**import-source** [**acl** *acl-number*]	Optional By default, all the (S, G) entries in the domain are advertised in the SA message.

Configuring a Rule for Filtering Received and Forwarded SA Messages

Besides the creation of source information, controlling multicast source information allows you to control the forwarding and reception of source information. You can control the reception of SA messages using the MSDP inbound filter (corresponding to the **import** keyword); you can control the forwarding of SA messages by using either the MSDP outbound filter (corresponding to the **export** argument) or the TTL threshold. By default, an MSDP peer receives and forwards all SA messages.

MSDP inbound/outbound filter implements the following functions:

- Filtering out all (S, G) entries
- Receiving/forwarding only the SA messages permitted by advanced ACL rules

An SA message carrying encapsulated data can reach the specified MSDP peer outside the domain only when the TTL in its IP header exceeds the threshold; therefore, you can control the forwarding of SA messages that carry encapsulated data by configuring the TTL threshold.

Table 391 Configure a rule for filtering received and forwarded SA messages

Operation	Command	Description
Enter system view	**system-view**	-
Enter MSDP view	**msdp**	-

Table 391 Configure a rule for filtering received and forwarded SA messages

Operation	Command	Description
Configure to filter SA messages to be received or forwarded	**peer** *peer-address* **sa-policy** { **import** | **export** } [**acl** *acl-number*]	Optional By default, no filtering is imposed on SA messages to be received or forwarded, namely all SA messages from MSDP peers are received or forwarded.
Configure the minimum TTL for the multicast packets sent to the specified MSDP peer	**peer** *peer-address* **minimum-ttl** *ttl-value*	Optional By default, the value of TTL threshold is 0.

Configuring SA Message Cache

With the SA message caching mechanism enabled on the router, the group that a new member subsequently joins can obtain all active sources directly from the SA cache and join the corresponding SPT source tree, instead of waiting for the next SA message.

You can configure the number of SA entries cached in each MSDP peer on the router by executing the following command, but the number must be within the system limit. The maximum number of cached SA messages on each MSDP peer and on all the MSDP peers on a router is limited by the system. To protect a router against Deny of Service (DoS) attacks, you can manually configure the maximum number of SA messages cached on the router. Generally, the configured number of SA messages cached should be less than the system limit.

Table 392 Configure SA message cache

Operation	Command	Description
Enter system view	**system-view**	-
Enter MSDP view	**msdp**	-
Enable SA message caching mechanism	**cache-sa-enable**	Optional By default, the SA message caching mechanism is enabled.
Configure the maximum number of SA messages cached	**peer** *peer-address* **sa-cache-maximum** *sa-limit*	Optional By default, the maximum number of SA messages cached on a router is 2,048.

Displaying and Debugging MSDP Configuration

Displaying and debugging MSDP configuration

After the above-mentioned configuration, you can use the **display** command in any view to display the MSDP running information, so as to verify configuration.

In user view, you can execute the **reset** command to reset the MSDP counter.

Table 393 Display and debug MSDP configuration

Operation	Command
Display the brief information of MSDP peer state	**display msdp brief**
Display the detailed information of MSDP peer status	**display msdp peer-status** [*peer-address*]

Table 393 Display and debug MSDP configuration

Operation	Command
Display the (S, G) state learned from MSDP peers	**display msdp sa-cache** [*group-address* | [*source-address*]] [*autonomous-system-number*]
Display the number of sources and groups in the MSDP cache	**display msdp sa-count** [*autonomous-system-number*]
Reset the TCP connection with the specified MSDP peer	**reset msdp peer** *peer-address*
Clear the cached SA messages	**reset msdp sa-cache** [*group-address*]
Clear the statistics information of the specified MSDP peer without resetting the MSDP peer	**reset msdp statistics** [*peer-address*]

Tracing the transmission path of an SA message over the network

You can use the **msdp-tracert** command in any view to trace the path along which the multicast data travels from the multicast source to the destination receiver over the network, so as to locate errors, if any.

Table 394 Trace the transmission path of an SA message over the network

Operation	Command
Trace the transmission path of an SA message over the network	**msdp-tracert** *source-address group-address rp-address* [**max-hops** *max-hops*] [**next-hop-info** | **sa-info** | **peer-info**]* [**skip-hops** *skip-hops*]

You can locate message loss and configuration errors by tracing the network path of the specified (S, G, RP) entries. Once the transmission path of SA messages is determined, correct configuration can prevent the flooding of SA messages.

MSDP Configuration Example

Configuration Example of MSDP Based on BGP Routes

Network requirements

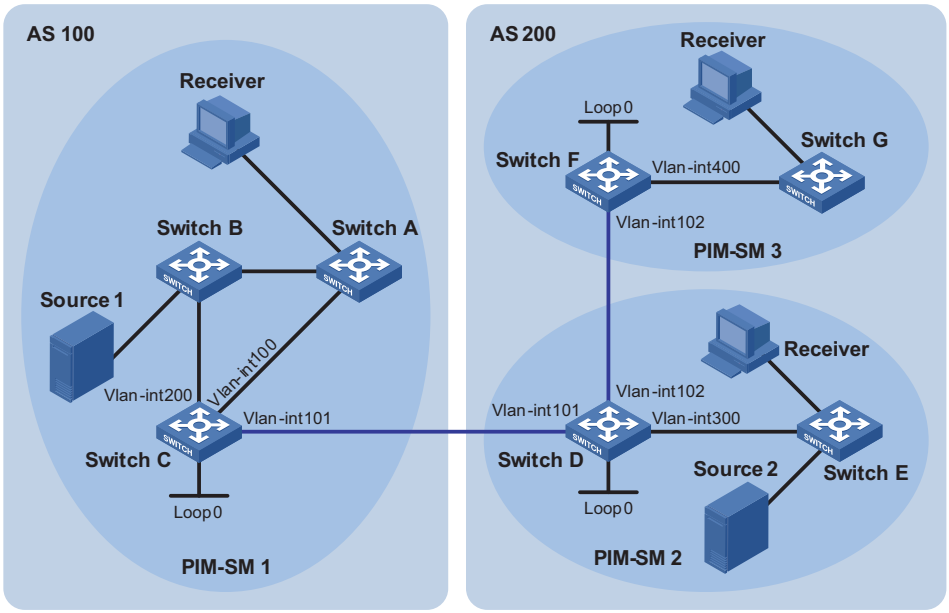
Two ISPs maintains their ASs, AS 100 and AS 200 respectively. OSPF is running within each AS, and BGP is running between the two ASs. PIM-SM1 belongs to AS 100, while PIM-SM2 and PIM-SM3 belong to AS 200.

Suppose each PIM-SM domain is a single-BSR-managed domain, having 0 or 1 multicast source S and multiple receivers. OSPF runs within each domain to provide unicast routes. An MSDP peering relationship is established between the RPs based on BGP routes within each PIM-SM network.

Loopback 0 on Switch C, Switch D and Switch E functions as the C-BSR and C-RP of its own PIM-SM domain respectively. An MSDP peering relationship is established between Switch C and Switch F based on EBGP routes, and an MSDP peering relationship is established between Switch F and Switch D based on IBGP routes.

Network diagram

Figure 124 Network diagram for MSDP configuration



Device	Interface	IP address	Device	Interface	IP address
Switch C	Vlan-int100	10.110.1.1/8	Switch D	Vlan-int300	10.110.4.1/8
	Vlan-int200	10.110.2.1/8		Vlan-int102	192.168.3.1/24
	Vlan-int101	192.168.1.1/24		Vlan-int101	192.168.1.2/24
	Loop0	1.1.1.1/32		Loop0	2.2.2.2/32
Switch F	Vlan-int400	10.110.3.1/8			
	Vlan-int102	192.168.3.2/24			
	Loop0	3.3.3.3/32			

Configuration procedure

1 Configure interface IP addresses and unicast routing protocol on the switches.

In each PIM-SM domain, configure the interface IP addresses on the switches and interconnect the switches through OSPF. Make sure that Switch A, Switch B and Switch C in the PIM-SM 1 domain are interoperable on the network layer, Switch D and Switch E in the PIM-SM 2 domain are interoperable on the network layer, and Switch F and Switch G in the PIM-SM 3 domain are interoperable on the network layer. On the other hand, switches in each PIM-SM domain can update routes dynamically by using unicast routing protocols. Configure the IP address and mask of each interface according to Figure 124. The details are omitted here.

2 Enable multicast and enable PIM-SM on each interface.

Enable multicast on SwitchC and enable PIM-SM on all interfaces. Switch C is taken for example. The configuration procedures on other switches are similar to that on Switch C. The details are omitted here.

```
<SwitchC> system-view
[SwitchC] multicast routing-enable
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] pim sm
[SwitchC-Vlan-interface100] quit
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] pim sm
[SwitchC-Vlan-interface200] quit
[SwitchC] interface vlan-interface 101
[SwitchC-Vlan-interface101] pim sm
[SwitchC] interface loopback 0
[SwitchC-LoopBack0] pim sm
[SwitchC-LoopBack0] quit
```

Configure the PIM domain boundary on Switch C, Switch D and Switch F respectively. Switch C is taken for example. The configuration procedures on Switch D and Switch F are similar to that on Switch C. The details are omitted here.

```
[SwitchC-Vlan-interface110] pim bsr-boundary
[SwitchC-Vlan-interface110] quit
```

3 Configure the interface Loopback0 and the location of C-BSRs and C-RPs.

Configure the interface Loopback0 on Switch C, Switch D, and Switch F and configure the locations of C-BSRs and C-RPs. Switch C is taken for example. The configuration procedures on Switch D and Switch F are similar to that on Switch C. The details are omitted here.

```
[SwitchC] pim
[SwitchC-pim] c-bsr loopback 0 32
[SwitchC-pim] c-rp loopback 0
[SwitchC-pim] quit
```

4 Configure BGP routes between ASs

Configure EBGP on Switch C, and import OSPF routes.

```
[SwitchC] router id 1.1.1.1
[SwitchC] bgp 100
[SwitchC-bgp] group as200 external
[SwitchC-bgp] peer as200 as-number 200
[SwitchC-bgp] peer 192.168.1.2 group as200
[SwitchC-bgp] import-route ospf
[SwitchC-bgp] quit
```

Configure IBGP and EBGP on Switch D, and import OSPF routes.

```
[SwitchD] router id 2.2.2.2
[SwitchD] bgp 200
[SwitchD-bgp] group as100 external
[SwitchD-bgp] peer as100 as-number 100
[SwitchD-bgp] peer 192.168.1.1 group as100
[SwitchD-bgp] group as200
[SwitchD-bgp] peer 192.168.3.2 group as200
[SwitchD-bgp] import-route ospf
[SwitchD-bgp] quit
```

Configure IBGP on Switch F, and import OSPF routes.

```
[SwitchF] router id 3.3.3.3
[SwitchF] bgp 200
[SwitchF-bgp] group as200
[SwitchF-bgp] peer as200 as-number 200
[SwitchF-bgp] peer 192.168.3.1 group as200
[SwitchF-bgp] import-route ospf
[SwitchF-bgp] quit
```

Carry out the **display bgp peer** command to view the BGP peering relationships between the switches. The information about BGP peering relationships between Switch C, Switch D and Switch F is displayed as follows:

```
[SwitchC] display bgp peer
 Peer        AS-num Ver Queued-Tx    Msg-Rx    Msg-Tx    Up/Down  State
------------------------------------------------------------------------------
192.168.1.2     200  4          0         24        21   00:41:00 Established
[SwitchF] display bgp peer
 Peer        AS-num Ver Queued-Tx    Msg-Rx    Msg-Tx    Up/Down  State
------------------------------------------------------------------------------
192.168.3.2     200  4          0         21        20   00:46:00 Established
[SwitchD] display bgp peer
    Peer        AS-num Ver Queued-Tx    Msg-Rx    Msg-Tx    Up/Down  State
------------------------------------------------------------------------------
192.168.1.1       100  4          0          1          4   00:01:05 Established
192.168.3.1      200  4          0          0          0   00:00:05 Active
```

Carry out the **display bgp routing-table** command to view the BGP routing table information on the switches. The BGP routing table information on Switch D is as follows:

```
[SwitchD] display bgp routing-table
Flags:   # - valid       ^ - active      I - internal
         D - damped      H - history     S - aggregate suppressed

    Dest/Mask          Next-hop        Med        Local-pref Origin As-path
------------------------------------------------------------------------------
#^  192.168.0.0        0.0.0.0         0                     IGP      100
#   1.1.1.1/32         192.168.1.1     0                     IGP      100
# I  2.2.2.2/32        192.168.3.1     0          100        IGP      100
#   3.3.3.3/32         0.0.0.0         0                     IGP      100
#   192.168.1.0        0.0.0.0         0                     IGP      100
#                      192.168.1.1     0                     IGP      100
#   192.168.1.1/32     0.0.0.0         0                     IGP      100
#   192.168.1.2/32     0.0.0.0         0                     IGP      100
#                      192.168.1.1     0                     IGP      100
#   192.168.3.0        0.0.0.0         0                     IGP      100
# I                    192.168.3.1     0          100        IGP      100
#   192.168.3.1/32     0.0.0.0         0                     IGP      100
#   192.168.3.2/32     0.0.0.0         0                     IGP      100
# I                    192.168.3.1     0          100        IGP      100
```

5 Configure MSDP peers

Configure an MSDP peer on Switch C.

```
[SwitchC] msdp
[SwitchC-msdp] peer 192.168.1.2 connect-interface Vlan-interface110
[SwitchC-msdp] quit
```

Configure an MSDP peer on Switch F.

```
[SwitchF] msdp
[SwitchF-msdp] peer 192.168.3.2 connect-interface Vlan-interface101
[SwitchF-msdp] quit
```

Configure MSDP peers on Switch D.

```
[SwitchD] msdp
[SwitchD-msdp] peer 192.168.1.1 connect-interface Vlan-interface110
[SwitchD-msdp] peer 192.168.3.1 connect-interface Vlan-interface101
[SwitchD-msdp] quit
```

When the multicast source S1 in PIM-SM1 sends multicast information, receivers in PIM-SM2 and PIM-SM3 can receive the multicast data. You can use the **display msdp brief** command to view the brief information of MSDP peering relationships between the switches. The brief information about MSDP peering relationships between Switch C, Switch D and Switch F is as follows:

```
[SwitchC] display msdp brief
MSDP Peer Brief Information
  Peer's Address     State     Up/Down time    AS     SA Count   Reset Count
  192.168.1.2        Up        00:12:27        200    13          0
[SwitchF] display msdp brief
MSDP Peer Brief Information
  Peer's Address     State     Up/Down time    AS     SA Count   Reset Count
  192.168.3.2        Up        00:15:32        200    8           0
[SwitchD] display msdp brief
MSDP Peer Brief Information
  Peer's Address     State     Up/Down time    AS     SA Count   Reset Count
  192.168.3.1        UP        01:07:08        200    8           0
  192.168.1.1        UP        00:06:39        100    13          0
```

View the detailed MSDP peer information on Switch F.

```
[SwitchC] display msdp peer-status
  MSDP Peer 192.168.1.2, AS 200
  Description:
  Information about connection status:
    State: Up
    Up/down time: 00:15:47
    Resets: 0
    Connection interface: Vlan-interface110 (192.168.1.1)
    Number of sent/received messages: 16/16
    Number of discarded output messages: 0
    Elapsed time since last connection or counters clear: 00:17:51
  Information about (Source, Group)-based SA filtering policy:
    Import policy: none
    Export policy: none
  Information about SA-Requests:
    Policy to accept SA-Request messages: none
    Sending SA-Requests status: disable
  Minimum TTL to forward SA with encapsulated data: 0
  SAs learned from this peer: 0, SA-cache maximum for the peer: none
  Input queue size: 0, Output queue size: 0
  Counters for MSDP message:
    Count of RPF check failure: 0
    Incoming/outgoing SA messages: 0/0
    Incoming/outgoing SA requests: 0/0
    Incoming/outgoing SA responses: 0/0
    Incoming/outgoing data packets: 0/0
```

Configuration Example of Anycast RP Application

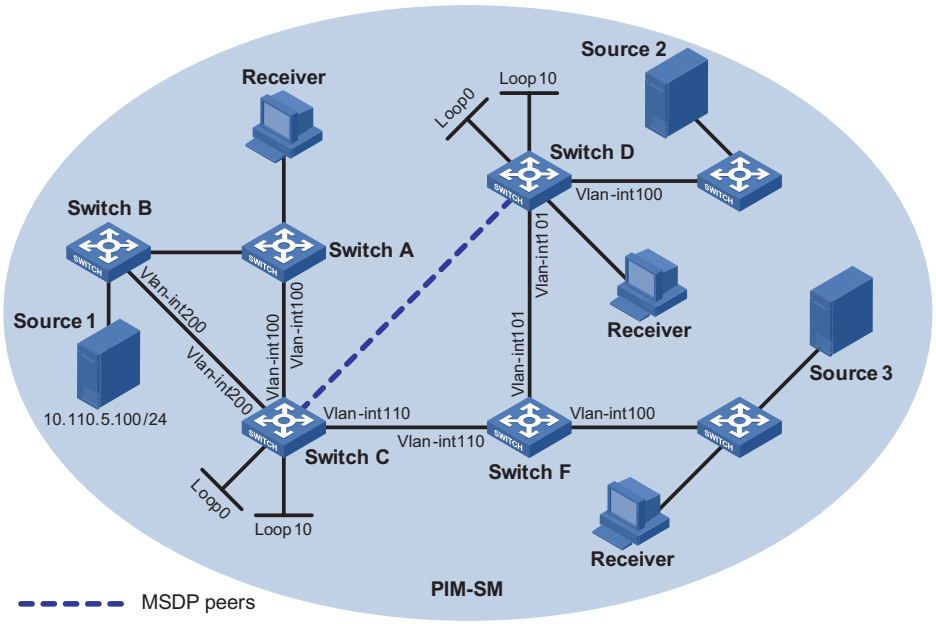
Network requirements

Each PIM-SM network is a single-BSR administrative domain, with multiple multicast sources (S) and receivers. With Anycast RP configured in each PIM-SM domain, when a new member joins the multicast group, the switch directly connected to the receiver can send a Join message to the nearest RP on the topology.

The PIM-SM network implements OSPF to provide unicast routes and establish MSDP peering relationship between Switch C and Switch D. Meanwhile, the Loopback10 interfaces of Switch C and Switch D play the roles of C-BSR and C-RP.

Network diagram

Figure 125 Network diagram for Anycast RP configuration



Device	Interface	IP address	Device	Interface	IP address
Switch A	Vlan-int100	10.110.1.2/24	Switch D	Vlan-int100	10.110.3.1/24
Switch B	Vlan-int200	10.110.2.2/24		Vlan-int101	192.168.3.2/24
Switch C	Vlan-int100	10.110.1.1/24		Loop0	2.2.2.2/32
	Vlan-int200	10.110.2.1/24		Loop10	10.1.1.1/32
	Vlan-int110	192.168.1.1/24	Switch F	Vlan-int100	10.110.4.1/24
	Loop0	1.1.1.1/32		Vlan-int101	192.168.3.1/24
	Loop10	10.1.1.1/32		Vlan-int110	192.168.1.2/24

Configuration procedure

1 Configure interface IP addresses and unicast routing protocols on the switches.

In the PIM-SM domain, configure the interface IP addresses on the switches and interconnect the switches through OSPF. Configure the IP address and mask of each interface according to Figure 125. The details are omitted here.

2 Enable multicast and configure PIM-SM.

Enable multicast on SwitchC and enable PIM-SM on all interfaces. The configuration procedures on other switches are similar to that on SwitchC. The details are omitted here.

```
<SwitchC> system-view
[SwitchC] multicast routing-enable
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] pim sm
[SwitchC-Vlan-interface100] quit
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] pim sm
[SwitchC-Vlan-interface200] quit
[SwitchC] interface vlan-interface 110
[SwitchC-Vlan-interface110] pim sm
[SwitchC-Vlan-interface110] quit
[SwitchC] interface loopback 0
[SwitchC-LoopBack0] pim sm
[SwitchC-LoopBack0] quit
[SwitchC] interface loopback 10
[SwitchC-LoopBack10] pim sm
[SwitchC-LoopBack10] quit
```

Configure the same Loopback10 interface address on SwitchC and SwitchD and configure the locations of C-BSRs and C-RPs. The configuration procedure on SwitchD is similar to that on SwitchC. The details are omitted here.

```
[SwitchC] pim
[SwitchC-pim] c-bsr loopback 10 32
[SwitchC-pim] c-rp loopback 10
[SwitchC-pim] quit
```

When the multicast source S1 in the PIM-SM domain sends multicast information, receivers on Switch D can receive multicast information. Carry out the **display pim routing-table** command to view PIM routes on the switch. The information about PIM routes on Switch C and Switch D is displayed as follows:

```
[SwitchC] display pim routing-table
PIM-SM Routing Table
Total 0 (*,*,RP)entry, 0 (*,G)entry, 2 (S,G)entries
 (10.110.5.100, 225.1.1.1), RP: 10.1.1.1 (local)
     Protocol 0x20: PIMSM, Flag 0x4: SPT
     UpTime: 00:10:20 , never timeout
     Upstream interface: Vlan-interface200,RPF neighbor: Vlan-interface200
Downstream interface list:
    1 oifs
      Vlan-interface110, Protocol 0x1: IGMP, never timeout
Matched 0 (S,G) entry, 0 (*,G) entries, 1 (*,*,RP) entry
[SwitchD] display pim routing-table
PIM-SM Routing Table
Total 0 (*,*,RP)entry, 0 (*,G)entry, 2 (S,G)entries
(10.110.5.100, 225.1.1.1), RP: 10.1.1.1
     Protocol 0x20: PIMSM, Flag 0x4: SPT
     UpTime: 00:03:32
     Upstream interface: Vlan-interface101,RPF neighbor: 192.168.3.2
Downstream interface list:
    1 oifs
      Vlan-interface100, Protocol 0x1: IGMP, never timeout
Matched 0 (S,G) entry, 0 (*,G) entries, 1 (*,*,RP) entry
```

3 Configure an MSDP peer.

Configure an MSDP peer on Loopback0 on SwitchC.

```
[SwitchC] msdp
[SwitchC-msdp] originating-rp loopback0
[SwitchC-msdp] peer 2.2.2.2 connect-interface loopback0
[SwitchC-msdp] quit
```

Configure an MSDP peer on Loopback0 on SwitchD.

```
[SwitchD] msdp
[SwitchD-msdp] originating-rp loopback0
[SwitchD-msdp] peer 1.1.1.1 connect-interface loopback0
[SwitchD-msdp] quit
```

Carry out the **display msdp brief** command to view the MSDP peering relationship established between switches. The MSDP peering relationship established between Switch C and Switch D is displayed as follows:

```
[SwitchC] display msdp brief
MSDP Peer Brief Information
  Peer's Address     State     Up/Down time    AS     SA Count   Reset Count
  2.2.2.2            Up        00:10:17        ?      0          0
[SwitchD] display msdp brief
MSDP Peer Brief Information
  Peer's Address     State     Up/Down time    AS     SA Count   Reset Count
  1.1.1.1            Up        00:10:18        ?      0          0
```

Configuration Example of a PIM Stub Domain

Network requirements

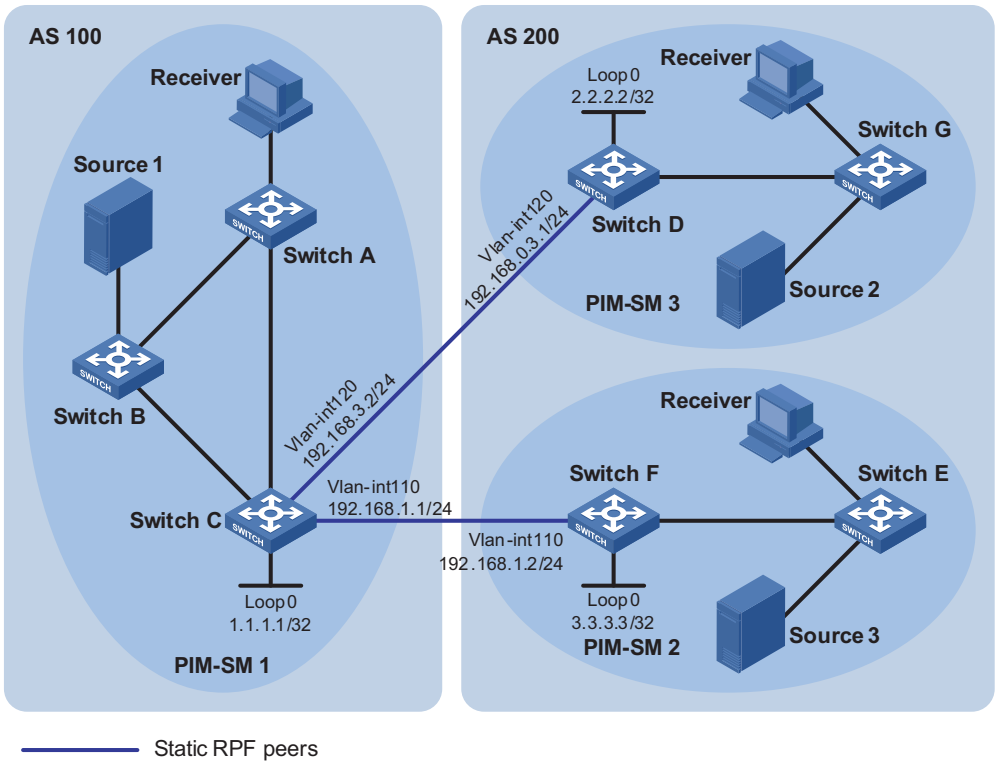
Two ISPs maintains their ASs, AS 100 and AS 200 respectively. OSPF is running within each AS, and BGP is running between the two ASs. PIM-SM1 belongs to AS 100, while PIM-SM2 and PIM-SM3 belong to AS 200.

Each PIM-SM domain is a single-BSR-managed domain, each having 0 or 1 multicast source S and multiple receivers. OSPF runs within each domain to provide unicast routes. PIM-SM2 and PIM-SM3 are both PIM stub domains, and BGP or MBGP is not required between these two domains and PIM-SM1. Instead, static RPF peers are configured to avoid RPF check on SA messages.

The respective Loopback0 of Switch C, Switch D and Switch F are configured as the C-BSR and C-RP of the respective PIM-SM domain. The static RPF peers of Switch C are Switch D and Switch F, while Switch C is the only RPF peer of Switch D and Switch F. Any switch can receive the SA messages sent by its static RPF peer(s) and permitted by the corresponding filtering policy.

Network diagram

Figure 126 Network diagram for static RPF peer configuration



Configuration procedure

1 Configure the interface IP addresses and unicast routing protocols for each switch

Configure interface IP addresses for each switch, and configure OSPF for interconnection between switches in each PIM-SM domain. Ensure the network-layer interoperation among switches in PIM-SM1, the network-layer interoperation between switches in PIM-SM2, and the network-layer interoperation between switches in PIM-SM3, and ensure the dynamic update of routing information between the switches in each PIM-SM domain is implemented through a unicast routing protocol. Configure the IP address and subnet mask for each interface as shown in Figure 126. The detailed configuration steps are omitted.

2 Enable multicast and enable PIM-SM on each interface.

Enable multicast on all the switches, and enable PIM-SM on each interface. The configuration procedures on the other switches are similar to the configuration procedure on Switch C. So the configuration procedures on the other switches are omitted.

```
[SwitchC] multicast routing-enable
[SwitchC] interface vlan-interface 100
[SwitchC-Vlan-interface100] pim sm
[SwitchC-Vlan-interface100] quit
[SwitchC] interface vlan-interface 200
[SwitchC-Vlan-interface200] pim sm
[SwitchC-Vlan-interface200] quit
```

```
[SwitchC] interface vlan-interface 110
[SwitchC-Vlan-interface110] pim sm
[SwitchC-Vlan-interface110] quit
[SwitchC] interface Vlan-interface 101
[SwitchC-Vlan-interface101] pim sm
[SwitchC-Vlan-interface101] quit
[SwitchC] interface loopback 0
[SwitchC-LoopBack0] pim sm
[SwitchC-LoopBack0] quit
```

Configure BSR administrative boundaries on Switch C, Switch D, and Switch F. The configuration procedures on Switch D and Switch F are similar to the configuration procedure on Switch C. So the configuration procedures are omitted.

```
[SwitchC-Vlan-interface101] pim bsr-boundary
[SwitchC-Vlan-interface101] quit
[SwitchC] interface vlan-interface 110
[SwitchC-Vlan-interface110] pim bsr-boundary
[SwitchC-Vlan-interface110] quit
```

3 Configure the location of the Loopback 0 interface, C-BSRs, and C-RPs.

Configure the location of the Loopback 0 interface, C-BSRs, and C-RPs on Switch C, Switch D, and Switch F respectively. The configuration procedures on Switch D and Switch F are similar to the configuration procedure on Switch C, so the configuration procedures are omitted.

```
[SwitchC] pim
[SwitchC-pim] c-bsr loopback 0 32
[SwitchC-pim] c-rp loopback 0
[SwitchC-pim] quit
```

4 Configure a static RPF peer

Configure Switch D and Switch F as static RPF peers of Switch C.

```
[SwitchC] ip ip-prefix list-df permit 192.168.0.0 16 greater-equal 1
6 less-equal 32
[SwitchC] msdp
[SwitchC-msdp] peer 192.168.3.1 connect-interface Vlan-interface101
[SwitchC-msdp] peer 192.168.1.2 connect-interface Vlan-interface110
[SwitchC-msdp] static-rpf-peer 192.168.3.1 rp-policy list-df
[SwitchC-msdp] static-rpf-peer 192.168.1.2 rp-policy list-df
[SwitchC-msdp] quit
```

Configure Switch C as static an RPF peer of Switch D and Switch F. The configuration procedure on Switch F is similar to the configuration procedure on Switch D, so the configuration procedure on Switch F is omitted.

```
[SwitchD] ip ip-prefix list-c permit 192.168.0.0 16 greater-equal 16
 less-equal 32
[SwitchD] msdp
[SwitchD-msdp] peer 192.168.3.2 connect-interface Vlan-interface101
[SwitchD-msdp] static-rpf-peer 192.168.3.2 rp-policy list-c
[SwitchD-msdp] quit
```

5 Verify the configuration

That no information is output after you carry out the **display bgp peer** command means that the BGP peering relationships are not established between the switches. When the multicast source S1 in PIM-SM1 sends multicast information, receivers in PIM-SM2 and PIM-SM3 can receive the multicast data. You can use the **display msdp brief** command to view the brief information of MSDP peering relationships between the switches. The information about MSDP peering relationships on Switch C, Switch D and Switch F is as follows:

```
[SwitchC] display msdp brief
MSDP Peer Brief Information
  Peer's Address     State     Up/Down time    AS     SA Count   Reset Count
  2.2.2.2            UP        01:07:08        ?       8           0
  3.3.3.3            UP        00:16:39        ?       13          0
[SwitchD] display msdp brief
MSDP Peer Brief Information
  Peer's Address     State     Up/Down time    AS     SA Count   Reset Count
  1.1.1.1            UP        01:07:09        ?       8           0
[SwitchF] display msdp brief
MSDP Peer Brief Information
 Peer's Address     State     Up/Down time    AS     SA Count   Reset Count
  1.1.1.1            UP        00:16:40        ?       13          0
```

Troubleshooting MSDP Configuration

MSDP Peer Always in the Down State

Symptom

An MSDP peer is configured, but it is always in the down state.

Analysis

An MSDP peer relationship between the locally configured **connect-interface** interface address and the configured peer address is based on a TCP connection. If the address of local **connect-interface** interface is inconsistent with the peer address configured on the peer router, no TCP connection can be established. If there is no route between the two peers, no TCP connection can be established.

Solution

1. Check the connectivity of the route between the routers. Use the **display ip routing-table** command to check that the unicast route between the routers is correct.
2. Further check that a unicast route exists between two routers that will become MSDP peers and that the route leads to the two peers.
3. Check that the interface addresses of the MSDP peers are consistent. Use the **display current-configuration** command to check that the address of the local connect-interface interface is consistent with the address of the corresponding MSDP peer.

No SA Entry in the SA Cache of the Router

Symptom

An MSDP fails to send (S, G) forwarding entries through an SA message.

Analysis

You can use the **import-source** command to send the (S, G) entries of the local multicast domain to the neighboring MSDP peer through SA messages. The **acl**

keyword is optional. If you do not use this keyword, all (S, G) entries will be filtered out by default, that is, none of the (S, G) entries in the local multicast domain will be advertised. Before the **import-source** command is executed, the system will send all (S, G) entries in the local multicast domain. If the MSDP fails to send the (S, G) entries of the local multicast domain through SA messages, verify that the **import-source** command is configured correctly.

Solution

1. Check the connectivity of the route between the routers. Use the **display ip routing-table** command to check that the unicast route between the routers is correct.
2. Further check that a unicast route exists between two routers that will become MSDP peers and that the route leads to the two peers.
3. Verify the configuration of the **import-source** command and the corresponding ACL to ensure that the ACL rule filters the right (S, G) entries.

49 AAA & RADIUS & HWTACACS CONFIGURATION

Overview

Introduction to AAA

AAA is shortened from the three security functions: authentication, authorization and accounting. It provides a uniform framework for you to configure the three security functions to implement the network security management.

The network security mentioned here mainly refers to access control. It mainly controls:

- Which users can access the network,
- Which services the users can have access to,
- How to charge the users who are using network resources.

Accordingly, AAA provides the following services:

Authentication

AAA supports the following authentication methods:

- None authentication: Users are trusted and are not authenticated. Generally, this method is not recommended.
- Local authentication: User information (including user name, password, and attributes) is configured on this device. Local authentication is fast and requires lower operational cost. But the information storage capacity is limited by device hardware.
- Remote authentication: Users are authenticated remotely through the RADIUS protocol or HWTACACS protocol. This device (for example, a 3Com series switch) acts as the client to communicate with the RADIUS server or TACACS server. For RADIUS protocol, both standard and extended RADIUS protocols can be used.

Authorization

AAA supports the following authorization methods:

- Direct authorization: Users are trusted and directly authorized.
- Local authorization: Users are authorized according to the related attributes configured for their local accounts on the device.
- RADIUS authorization: Users are authorized after they pass the RADIUS authentication. The authentication and authorization of RADIUS protocol are bound together, and you cannot perform RADIUS authorization alone without RADIUS authentication.
- HWTACACS authorization: Users are authorized by TACACS server.

Accounting

AAA supports the following accounting methods:

- None accounting: No accounting is performed for users.
- Remote accounting: User accounting is performed on the remote RADIUS server or TACACS server.

Generally, AAA adopts the client/server structure, where the client acts as the managed resource and the server stores user information. This structure has good scalability and facilitates the centralized management of user information.

Introduction to ISP Domain

An Internet service provider (ISP) domain is a group of users who belong to the same ISP. For a user name in the format of *userid@isp-name*, the *isp-name* following the @ character is the ISP domain name. The access device uses *userid* as the user name for authentication, and *isp-name* as the domain name.

In a multi-ISP environment, the users connected to the same access device may belong to different domains. Since the users of different ISPs may have different attributes (such as different compositions of user name and password, different service types/rights), it is necessary to distinguish the users by setting ISP domains.

You can configure a set of ISP domain attributes (including AAA policy, RADIUS scheme, and so on) for each ISP domain independently in ISP domain view.

Introduction to RADIUS

AAA is a management framework. It can be implemented by not only one protocol. But in practice, the most commonly used protocol for AAA is RADIUS.

What is RADIUS

RADIUS (remote authentication dial-in user service) is a distributed information exchange protocol in client/server structure. It can prevent unauthorized access to the network and is commonly used in network environments where both high security and remote user access service are required.

The RADIUS service involves three components:

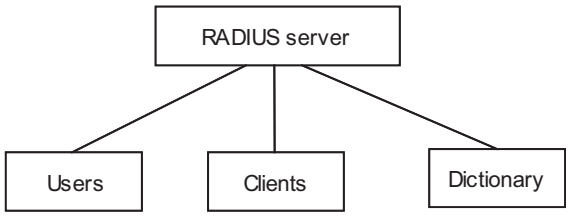
- Protocol: Based on the UDP/IP layer, RFC 2865 and 2866 define the frame format and message transfer mechanism of RADIUS, and define 1812 as the authentication port and 1813 as the accounting port.
- Server: The RADIUS server runs on a computer or workstation at the center. It stores and maintains the information on user authentication and network service access.
- Client: The RADIUS clients run on the dial-in access server device. They can be deployed anywhere in the network.

RADIUS is based on client/server model. Acting as a RADIUS client, the switch passes user information to a designated RADIUS server, and makes processing (such as connecting/disconnecting users) depending on the responses returned from the server. The RADIUS server receives user's connection requests, authenticates users, and returns all required information to the switch.

Generally, the RADIUS server maintains the following three databases (as shown in Figure 127):

- Users: This database stores information about users (such as user name, password, adopted protocol and IP address).
- Clients: This database stores the information about RADIUS clients (such as shared keys).
- Dictionary: This database stores the information used to interpret the attributes and attribute values of the RADIUS protocol.

Figure 127 Databases in RADIUS server

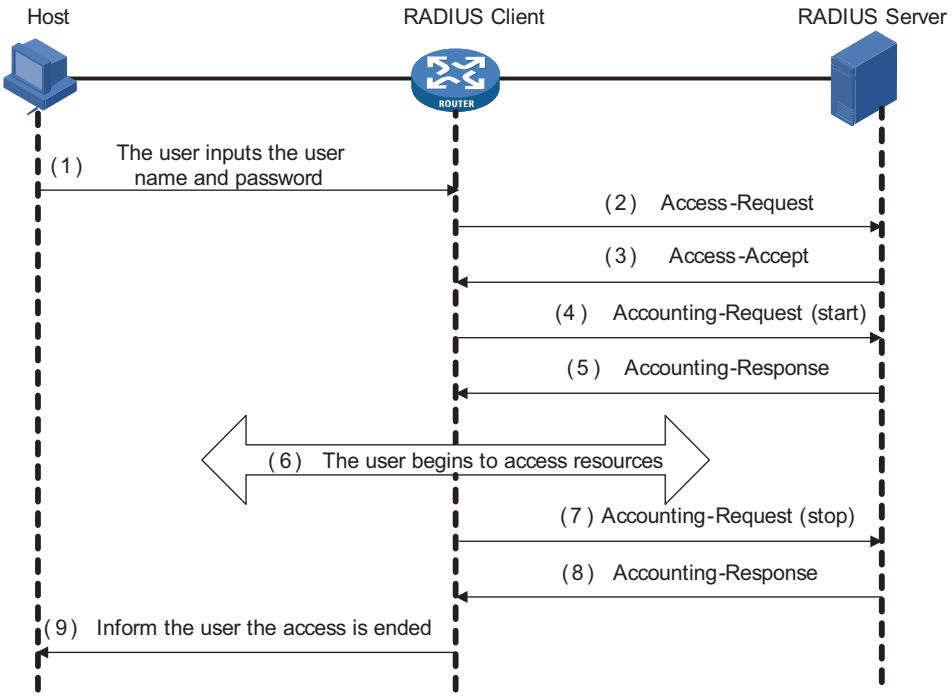


In addition, the RADIUS server can act as the client of some other AAA server to provide the authentication or accounting proxy service.

Basic message exchange procedure of RADIUS

The messages exchanged between a RADIUS client (a switch, for example) and the RADIUS server are verified by using a shared key. This enhances the security. The RADIUS protocol combines the authentication and authorization processes together by sending authorization information in the authentication response message. Figure 128 depicts the message exchange procedure between user, switch and RADIUS server.

Figure 128 Basic message exchange procedure of RADIUS



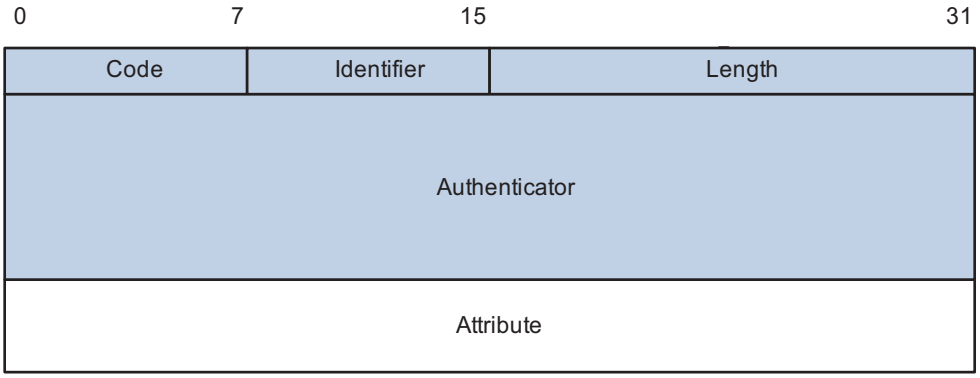
The basic message exchange procedure of RADIUS is as follows:

1. The user enters the user name and password.
2. The RADIUS client receives the user name and password, and then sends an authentication request (Access-Request) to the RADIUS server.
3. The RADIUS server compares the received user information with that in the Users database to authenticate the user. If the authentication succeeds, the RADIUS server sends back an authentication response (Access-Accept), which contains the information of user's rights, to the RADIUS client. If the authentication fails, it returns an Access-Reject response.
4. The RADIUS client accepts or denies the user depending on the received authentication result. If it accepts the user, the RADIUS client sends a start-accounting request (Accounting-Request, with the Status-Type filed set to "start") to the RADIUS server.
5. The RADIUS server returns a start-accounting response (Accounting-Response).
6. The user starts to access the resources.
7. The RADIUS client sends a stop-accounting request (Accounting-Request, with the Status-Type field set to "stop") to the RADIUS server.
8. The RADIUS server returns a stop-accounting response (Accounting-Response).
9. The resource access of the user is ended.

RADIUS packet structure

RADIUS uses UDP to transmit messages. It ensures the correct message exchange between RADIUS server and client through the following mechanisms: timer management, retransmission, and backup server. Figure 129 depicts the structure of the RADIUS packets.

Figure 129 RADIUS packet structure



1 The Code field decides the type of the RADIUS packet, as shown in Table 395.

Table 395 Description on major values of the Code field

Code	Packet type	Packet description
1	Access-Request	Direction: client->server. The client transmits this packet to the server to determine if the user can access the network. This packet carries user information. It must contain the User-Name attribute and may contain the following attributes: NAS-IP-Address, User-Password and NAS-Port.
2	Access-Accept	Direction: server->client. The server transmits this packet to the client if all the attribute values carried in the Access-Request packet are acceptable (that is, the user passes the authentication).
3	Access-Reject	Direction: server->client. The server transmits this packet to the client if any attribute value carried in the Access-Request packet is unacceptable (that is, the user fails the authentication).
4	Accounting-Request	Direction: client->server. The client transmits this packet to the server to request the server to start or end the accounting (whether to start or to end the accounting is determined by the Acct-Status-Type attribute in the packet). This packet carries almost the same attributes as those carried in the Access-Request packet.
5	Accounting-Response	Direction: server->client. The server transmits this packet to the client to notify the client that it has received the Accounting-Request packet and has correctly recorded the accounting information.

2 The Identifier field (one byte) identifies the request and response packets. It is subject to the Attribute field and varies with the received valid responses, but keeps unchanged during retransmission.

3 The Length field (two bytes) specifies the total length of the packet (including the Code, Identifier, Length, Authenticator and Attribute fields). The bytes beyond the length will be regarded as padding bytes and are ignored upon receiving the packet. If the received packet is shorter than the value of this field, it will be discarded.

4 The Authenticator field (16 bytes) is used to verify the packet returned from the RADIUS server; it is also used in the password hiding algorithm. There are two kinds of authenticators: Request and Response.

5 The Attribute field contains special authentication, authorization, and accounting information to provide the configuration details of a request or response packet. This field is represented by a field triplet (Type, Length and Value):

- The Type field (one byte) specifies the type of the attribute. Its value ranges from 1 to 255. Table 396 lists the attributes that are commonly used in RADIUS authentication and authorization.
- The Length field (one byte) specifies the total length of the Attribute field in bytes (including the Type, Length and Value fields).
- The Value field (up to 253 bytes) contains the information about the attribute. Its content and format are determined by the Type and Length fields.

Table 396 RADIUS attributes

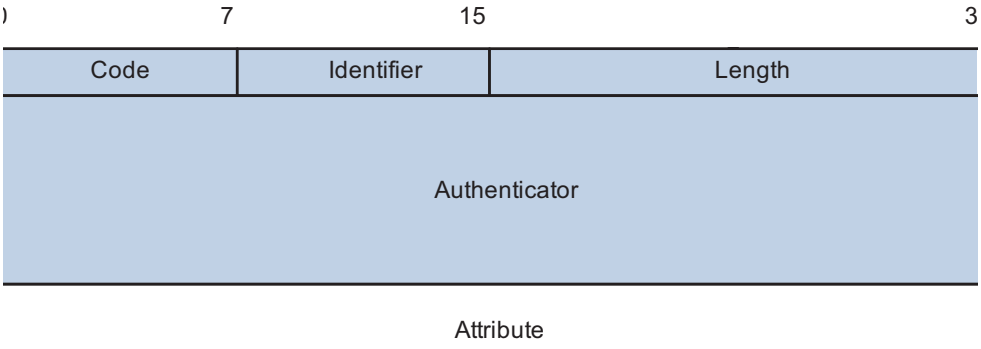
Value of the Type field	Attribute type	Value of the Type field	Attribute type
1	User-Name	23	Framed-IPX-Network
2	User-Password	24	State
3	CHAP-Password	25	Class
4	NAS-IP-Address	26	Vendor-Specific
5	NAS-Port	27	Session-Timeout
6	Service-Type	28	Idle-Timeout
7	Framed-Protocol	29	Termination-Action
8	Framed-IP-Address	30	Called-Station-Id
9	Framed-IP-Netmask	31	Calling-Station-Id
10	Framed-Routing	32	NAS-Identifier
11	Filter-ID	33	Proxy-State
12	Framed-MTU	34	Login-LAT-Service
13	Framed-Compression	35	Login-LAT-Node
14	Login-IP-Host	36	Login-LAT-Group
15	Login-Service	37	Framed-AppleTalk-Link
16	Login-TCP-Port	38	Framed-AppleTalk-Network
17	(unassigned)	39	Framed-AppleTalk-Zone
18	Reply-Message	40-59	(reserved for accounting)
19	Callback-Number	60	CHAP-Challenge
20	Callback-ID	61	NAS-Port-Type
21	(unassigned)	62	Port-Limit
22	Framed-Route	63	Login-LAT-Port

The RADIUS protocol takes good scalability. Attribute 26 (Vender-Specific) defined in this protocol allows a device vendor to extend RADIUS to implement functions that are not defined in standard RADIUS.

Figure 130 depicts the structure of attribute 26. The Vendor-ID field representing the code of the vendor occupies four bytes. The first byte is 0, and the other three bytes are defined in RFC1700. Here, the vendor can encapsulate multiple

customized sub-attributes (containing Type, Length and Value) to obtain extended RADIUS implementation.

Figure 130 Part of the RADIUS packet containing extended attribute



Introduction to HWTACACS

What is HWTACACS

HW Terminal Access Controller Access Control System (HWTACACS) is an enhanced security protocol based on TACACS (RFC1492). Similar to the RADIUS protocol, it implements AAA for different types of users (such as PPP/VPDN login users and terminal users) through communications with TACACS servers in the Client-Server mode.

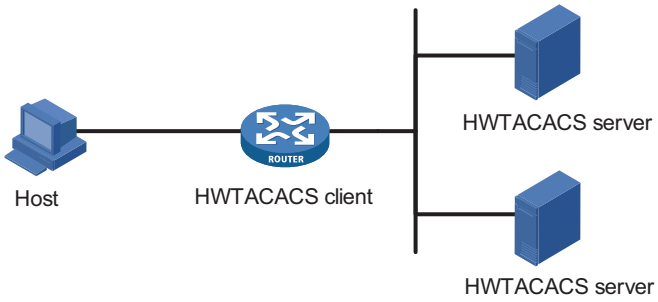
Compared with RADIUS, HWTACACS provides more reliable transmission and encryption, and therefore is more suitable for security control. Table 397 lists the primary differences between HWTACACS and RADIUS protocols.

Table 397 Comparison between HWTACACS and RADIUS

HWTACACS	RADIUS
Adopts TCP, providing more reliable network transmission.	Adopts UDP.
Encrypts the entire packet except the HWTACACS header.	Encrypts only the password field in authentication packets.
Separates authentication from authorization. For example, you can provide authentication and authorization on different TACACS servers.	Brings together authentication and authorization.
Suitable for security control.	Suitable for accounting.
Supports to authorize the use of configuration commands.	Not support.

In a typical HWTACACS application, a dial-up or terminal user needs to log in to the device for operations. As the client of HWTACACS in this case, the switch sends the username and password to the TACACS server for authentication. After passing authentication and being authorized, the user can log in to the switch to perform operations, as shown in Figure 131.

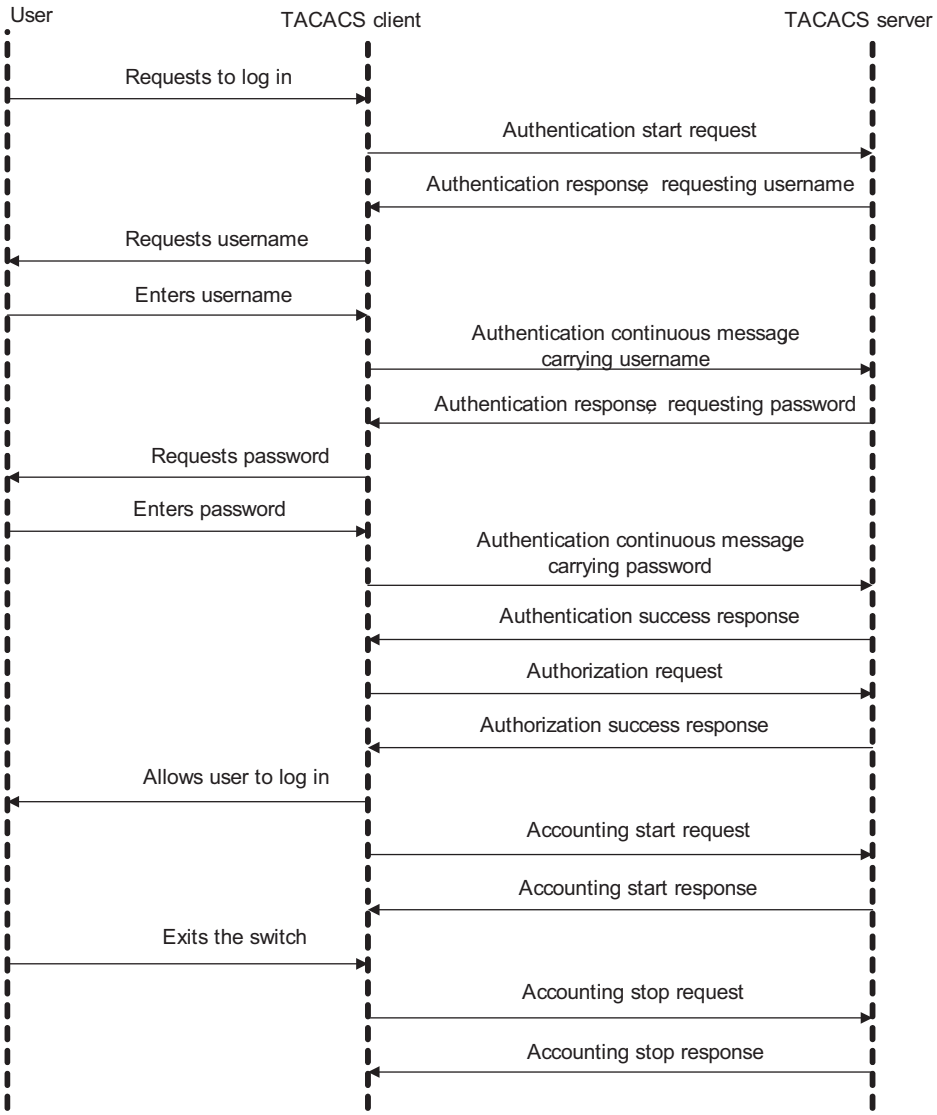
Figure 131 Network diagram for a typical HWTACACS application



Basic message exchange procedure in HWTACACS

For example, use HWTACACS to implement authentication, authorization, and accounting for a telnet user. Figure 132 illustrates the basic message exchange procedure:

Figure 132 The AAA implementation procedure for a telnet user



The basic message exchange procedure is as follows:

1. A user requests access to the switch; the TACACS client sends an authentication start request packet to TACACS server upon receipt of the request.
2. The TACACS server sends back an authentication response requesting for the username; the TACACS client asks the user for the username upon receipt of the response.
3. The TACACS client sends an authentication continuance packet carrying the username after receiving the username from the user.
4. The TACACS server sends back an authentication response, requesting for the password. Upon receipt of the response, the TACACS client requests the user for the login password.
5. After receiving the login password, the TACACS client sends an authentication continuance packet carrying the login password to the TACACS server.
6. The TACACS server sends back an authentication response indicating that the user has passed the authentication.
7. The TACACS client sends the user authorization request packet to the TACACS server.
8. The TACACS server sends back the authorization response, indicating that the user has passed the authorization.
9. Upon receipt of the response indicating an authorization success, the TACACS client pushes the configuration interface of the switch to the user.
10. The TACACS client sends an accounting start request packet to the TACACS server.
11. The TACACS server sends back an accounting response, indicating that it has received the accounting start request.
12. The user logs out; the TACACS client sends an accounting stop request to the TACACS server.
13. The TACACS server sends back an accounting stop packet, indicating that the accounting stop request has been received.

Configuration Tasks

Table 398 Configuration tasks

Operation		Description	Related section
AAA configuration	Create an ISP domain	Required	"Creating an ISP Domain" on page 518
	Configure the attributes of the ISP domain	Optional	"Configuring the Attributes of an ISP Domain" on page 519
	Configure an AAA scheme for the ISP domain	Required If local authentication is adopted, refer to "Configuring the Attributes of a Local User" on page 523. If RADIUS authentication is adopted, refer to "RADIUS Configuration" on page 525.	"Configuring an AAA Scheme for an ISP Domain" on page 520.
	Configure dynamic VLAN assignment	Optional	"Configuring Dynamic VLAN Assignment" on page 522.
	Configure the attributes of a local user	Optional	"Configuring the Attributes of a Local User" on page 523
	Cut down user connections forcibly	Optional	"Cutting Down User Connections Forcibly" on page 524

Table 398 Configuration tasks

Operation		Description	Related section
RADIUS configuration	Create a RADIUS scheme	Required	"Creating a RADIUS Scheme" on page 525
	Configure RADIUS authentication/authorization servers	Required	"Configuring RADIUS Authentication/Authorization Servers" on page 525
	Configure RADIUS accounting servers	Required	"Configuring RADIUS Accounting Servers" on page 526
	Configure shared keys for RADIUS packets	Optional	"Configuring Shared Keys for RADIUS Packets" on page 527
	Configure the maximum number of transmission attempts of RADIUS requests	Optional	"Configuring the Maximum Number of Transmission Attempts of RADIUS Requests" on page 528
	Configure the supported RADIUS server type	Optional	"Configuring the Supported RADIUS Server Type" on page 528
	Configure the status of RADIUS servers	Optional	"Configuring the Status of RADIUS Servers" on page 528
	Configure the attributes for data to be sent to RADIUS servers	Optional	"Configuring the Attributes for Data to be Sent to RADIUS Servers" on page 529
	Configure a local RADIUS authentication server	Optional	"Configuring a Local RADIUS Authentication Server" on page 530
	Configure the timers for RADIUS servers	Optional	"Configuring the Timers of RADIUS Servers" on page 530
	Configure the user re-authentication upon device restart function	Optional	"Configuring the User Re-Authentication upon Device Restart Function" on page 531

Table 398 Configuration tasks

Operation		Description	Related section
HWTACACS configuration	Create a HWTACACS scheme	Required	"Creating a HWTACACS Scheme" on page 532
	Configure HWTACACS authentication servers	Required	"Configuring HWTACACS Authentication Servers" on page 532
	Configure HWTACACS authorization servers	Required	"Configuring HWTACACS Authorization Servers" on page 533
	Configure HWTACACS accounting servers	Optional	"Configuring HWTACACS Accounting Servers" on page 533
	Configure shared keys for RADIUS packets	Optional	"Configuring Shared Keys for RADIUS Packets" on page 534
	Configure the attributes for data to be sent to TACACS servers	Optional	"Configuring the Attributes for Data to be Sent to TACACS Servers" on page 535
	Configure the timers of TACACS servers	Optional	"Configuring the Timers of TACACS Servers" on page 535

AAA Configuration

The goal of AAA configuration is to protect network devices against unauthorized access and at the same time provide network access services to authorized users. If you need to use ISP domains to implement AAA management on access users, you need to configure the ISP domains.

Configuration Prerequisites

If you want to adopt remote AAA method, you must create a RADIUS or HWTACACS scheme.

- RADIUS scheme (**radius-scheme**): You can reference a configured RADIUS scheme to implement AAA services. For the configuration of RADIUS scheme, refer to "RADIUS Configuration" on page 525.
- HWTACACS scheme (**hwtacacs-scheme**): You can reference a configured RADIUS scheme to implement AAA services. For the configuration of RADIUS scheme, refer to "HWTACACS Configuration" on page 532.

Creating an ISP Domain

Table 399 Create an ISP domain

Operation	Command	Description
Enter system view	**system-view**	-
Create an ISP domain and enter its view, enter the view of an existing ISP domain, or configure the default ISP domain	**domain** { *isp-name* | **default** { **disable** | **enable** *isp-name* } }	Required The default ISP domain is "system".

Configuring the Attributes of an ISP Domain

Table 400 Configure the attributes of an ISP domain

Operation	Command	Description
Enter system view	**system-view**	-
Create an ISP domain or enter the view of an existing ISP domain	**domain** *isp-name*	Required
Activate/deactivate the ISP domain	**state** { **active** | **block** }	Optional By default, once an ISP domain is created, it is in the **active** state and all the users in this domain are allowed to access the network.
Set the maximum number of access users that can be contained in the ISP domain	**access-limit** { **disable** | **enable** *max-user-number* }	Optional After an ISP domain is created, the number of access users it can contain is unlimited by default.
Set the user idle-cut function	**idle-cut** { **disable** | **enable** *minute flow* }	Optional By default, user idle-cut function is disabled.
Open/close the accounting-optional switch	**accounting optional**	Optional By default, once an ISP domain is created, the accounting-optional switch is closed.
Set the messenger function	**messenger time** { **enable** *limit interval* | **disable** }	Optional By default, the messenger function is disabled.
Set the self-service server location function	**self-service-url** { **disable** | **enable** *url-string* }	Optional By default, the self-service server location function is disabled.

CAUTION:

- *On a Switch 7750, each access user belongs to an ISP domain. You can configure up to 16 ISP domains on the switch. When a user logs in, if no ISP domain name is carried in the user name, the switch assumes that the user belongs to the default ISP domain.*
- *When charging a user, if the system does not find any available accounting server or fails to communicate with any accounting server, it will not disconnect the user as long as the* ***accounting optional*** *command has been executed.*
- *The self-service server location function must cooperate with a self-service-supported RADIUS server (such as CAMS). Through self-service, users can manage and control their accounts or module numbers by themselves. A server installed with the self-service software is called a self-service server.*

3Com's CAMS Server is a service management system used to manage networks and secure networks and user information. Cooperating with other network devices (such as switches) in a network, the CAMS Server implements the AAA (authentication, authorization and accounting) services and rights management.

Configuring an AAA Scheme for an ISP Domain

You can configure an AAA scheme in one of the following two ways:

Configuring a bound AAA scheme

You can use the **scheme** command to specify an AAA scheme. If you specify a RADIUS or HWTACACS scheme, the authentication, authorization and accounting will be uniformly implemented by the RADIUS server or TACACS server specified in the RADIUS or HWTACACS scheme. In this way, you cannot specify different schemes for authentication, authorization and accounting respectively.

Table 401 Configure an AAA scheme for an ISP domain

Operation	Command	Description
Enter system view	**system-view**	-
Create an ISP domain or enter the view of an existing ISP domain	**domain** *isp-name*	Required
Configure an AAA scheme for the ISP domain	**scheme** { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] | **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] }	Required By default, the ISP domain uses the **local** AAA scheme.
Configure an RADIUS scheme for the ISP domain	**radius-scheme** *radius-scheme-name*	Optional This function can also be implemented by using the **scheme** command to specify the RADIUS scheme to be used.

CAUTION:

- *You can execute the **scheme** command with the radius-scheme-name argument to adopt an already configured RADIUS scheme to implement all the three AAA functions. If you adopt the local scheme, only the authentication and authorization functions are implemented, the accounting function cannot be implemented.*
- *If you execute the **scheme radius-scheme** radius-scheme-name **local** command, the local scheme becomes the secondary scheme in case the RADIUS server does not response normally. That is, if the communication between the switch and the RADIUS server is normal, no local authentication is performed; otherwise, local authentication is performed.*
- *If you execute the **scheme hwtacacs-scheme** radius-scheme-name **local** command, the local scheme becomes the secondary scheme in case the TACACS server does not respond normally. That is, if the communication between the switch and the TACACS server is normal, no local authentication is performed; otherwise, local authentication is performed.*
- *If you adopt **local** or **none** as the primary scheme, the local authentication is performed or no authentication is performed. In this case, you cannot perform RADIUS authentication at the same time.*

Configuring separate AAA schemes

You can use the **authentication**, **authorization**, and **accounting** commands to specify a scheme for each of the three AAA functions (authentication, authorization and accounting) respectively. The following gives the implementations of this separate way for the services supported by AAA.

- For terminal users

Authentication: RADIUS, local, HWTACACS, or none.

Authorization: none or HWTACACS

Accounting: RADIUS, HWTACACS or none.

You can configure combined authentication, authorization and accounting schemes by using the above implementations.

- For FTP users

Only authentication is supported for FTP users.

Authentication: RADIUS, local, or HWTACACS.

Perform the following configuration in ISP domain view.

Table 402 Configure separate AAA schemes

Operation	Command	Description
Enter system view	**system-view**	-
Create an ISP domain or enter the view of an existing ISP domain	**domain** *isp-name*	Required
Configure an authentication scheme for the ISP domain	**authentication** { **radius-scheme** *radius-scheme-name* [**local**] | **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** }	Optional By default, no separate authentication scheme is configured.
Configure an authorization scheme for the ISP domain	**authorization** { **none** | **hwtacacs-scheme** *hwtacacs-scheme-name* }	Optional By default, no separate authorization scheme is configured.
Configure an accounting scheme for the ISP domain	**accounting** { **none** | **radius-scheme** *radius-scheme-name* | **hwtacacs-scheme** *hwtacacs-scheme-name* }	Optional By default, no separate accounting scheme is configured.



- *If a bound AAA scheme is configured as well as the separate authentication, authorization and accounting schemes, the separate ones will be adopted in precedence.*
- *RADIUS scheme and local scheme do not support the separation of authentication and authorization. Therefore, pay attention when you make*

*authentication and authorization configuration for a domain: if the **scheme radius-scheme** or **scheme local** command is executed, the **authorization none** command is executed, while the **authentication** command is not executed, the authorization information returned from the RADIUS or local scheme still takes effect.*

Configuring Dynamic VLAN Assignment

The dynamic VLAN assignment feature enables a switch to dynamically add the switch ports of successfully authenticated users to different VLANs according to the attributes assigned by the RADIUS server, so as to control the network resources that different users can access.

Currently, the switch supports the RADIUS authentication server to assign the following two types of VLAN IDs: integer and string.

- Integer: If the RADIUS server assigns integer type of VLAN IDs, you can set the VLAN assignment mode to integer on the switch (this is also the default mode on the switch). Then, upon receiving an integer ID assigned by the RADIUS authentication server, the switch adds the port to the VLAN whose VLAN ID is equal to the assigned integer ID. If no such a VLAN exists, the switch first creates a VLAN with the assigned ID, and then adds the port to the newly created VLAN.
- String: If the RADIUS server assigns string type of VLAN IDs, you can set the VLAN assignment mode to string on the switch. Then, upon receiving a string ID assigned by the RADIUS authentication server, the switch compares the ID with existing VLAN names on the switch. If it finds a match, it adds the port to the corresponding VLAN. Otherwise, the VLAN assignment fails and the user cannot pass the authentication.

The switch supports the integer mode and string mode of dynamic VLAN assignments to adapt to authentication server. Different servers assign VLANs in different ways. You are recommended to configure the switch based on the mode of dynamic VLAN assignment used by the server.

Table 403 Common VLAN assignment modes for RADIUS server

Server type	Dynamic VLAN assignment mode
CAMS	Integer (For the latest version, whether the mode is integer or string depends on attribute value.)
ACS	String
FreeRADIUS	Determined by attribute value (A value of 100 represents the integer mode and a value of "100" represents the string mode).
Shiva Access Manager	String
Steel-Belted Radius Administrator	String

In actual applications, to use this feature together with Guest VLAN, you should better set port control to port-based mode.

Table 404 Configure dynamic VLAN assignment

Operation	Command	Description
Enter system view	**system-view**	-

Table 404 Configure dynamic VLAN assignment

Operation	Command	Description
Create an ISP domain and enter its view	**domain** *isp-name*	-
Set the VLAN assignment mode	**vlan-assignment-mode** { **integer** | **string** }	Optional By default, the VLAN assignment mode is integer.
Create a VLAN and enter its view	**vlan** *vlan-id*	-
Set a VLAN name for VLAN assignment	**name** *string*	This operation is required if the VLAN assignment mode is set to string.

CAUTION:

- *In string mode, if the VLAN ID assigned by the RADIUS server is a character string containing only digits (for example, 1024), the switch first regards it as an integer VLAN ID: the switch transforms the string to an integer value and judges if the value is in the valid VLAN ID range; if it is, the switch adds the authenticated port to the VLAN with the integer value as the VLAN ID (VLAN 1024, for example).*
- *To implement dynamic VLAN assignment on a port where both MSTP and 802.1x are enabled, you must set the MSTP port to an edge port.*

Configuring the Attributes of a Local User

When **local** scheme is chosen as the AAA scheme, you should create local users on the switch and configure the relevant attributes.

The local users are users set on the switch, with each user uniquely identified by a user name. To make a user who is requesting network service pass through the local authentication, you should add an entry in the local user database on the switch for the user.

Table 405 Configure the attributes of a local user

Operation	Command	Description
Enter system view	**system-view**	-
Add a local user and enter local user view	**local-user** *user-name*	Required By default, there is no local user in the system.
Set a password for the specified user	**password** { **simple** | **cipher** } *password*	Optional
Set the password display mode of all local users	**local-user password-display-mode** { **cipher-force** | **auto** }	Optional By default, the password display mode of all access users is **auto**, indicating the passwords of access users are displayed in the modes set with the **password** command.
Set the state of the specified user	**state** { **active** | **block** }	Optional By default, the local users are in the **active** state once they are created, that is, they are allowed to request network services.

Table 405 Configure the attributes of a local user

Operation	Command	Description
Authorize the user to access the specified type(s) of service(s)	**service-type** { **ftp** | **lan-access** | { **telnet** | **ssh** | **terminal** }* [**level** *level*] }	Required By default, the system does not authorize the user to access any service.
Set the priority level of the user	**level** *level*	Optional By default, the priority level of the user is 0.
Set the attributes of the user whose service type is lan-access	**attribute** { **ip** *ip-address* | **mac** *mac-address* | **idle-cut** *second* | **access-limit** *max-user-number* | **vlan** *vlan-id* | **location** { **nas-ip** *ip-address* **port** *port-number* | **port** *port-number* } }*	Optional If the user is bound to a remote port, you must specify the **nas-ip** parameter (the following *ip-address* is 127.0.0.1 by default, representing this device). If the user is bound to a local port, you do not need to specify the **nas-ip** parameter.

CAUTION:

- *The character string of user-name cannot contain "/", ":", "*", "?", "<" and ">". Moreover, "@" can be used no more than once.*
- *After the **local-user password-display-mode cipher-force** command is executed, all passwords will be displayed in cipher mode even through you specify to display user passwords in plain text by using the **password** command.*
- *If the configured authentication method (local or RADIUS) requires a user name and a password, the command level that a user can access after login is determined by the priority level of the user. For SSH users, when they use RSA shared keys for authentication, the commands they can access are determined by the levels set on their user interfaces.*
- *If the configured authentication method is none or requires a password, the command level that a user can access after login is determined by the level of the user interface.*

Cutting Down User Connections Forcibly

Table 406 Cut down user connection forcibly

Operation	Command	Description
Enter system view	**system-view**	-
Cut down user connections forcibly	**cut connection** { **all** | **access-type** { **dot1x** | **mac-authentication** } | **domain** *isp-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **radius-scheme** *radius-scheme-name* | **vlan** *vlan-id* | **ucibindex** *ucib-index* | **user-name** *user-name* }	Required

*Telnet and FTP users can use the **display connection** command to view the connection, but they cannot use the **cut connection** command to cut down the connection.*

RADIUS Configuration

The RADIUS protocol configuration is performed on a RADIUS scheme basis. In an actual network environment, you can either use a single RADIUS server or two RADIUS servers (primary and secondary servers with the same configuration but different IP addresses) in a RADIUS scheme. After creating a new RADIUS scheme, you should configure the IP address and UDP port number of each RADIUS server you want to use in this scheme. These RADIUS servers fall into two types: authentication/authorization, and accounting. And for each kind of server, you can configure two servers in a RADIUS scheme: primary server and secondary server. A RADIUS scheme has the following attributes: IP addresses of the primary and secondary servers, shared keys, and types of the RADIUS servers.

In an actual network environment, you can configure the above parameters as required. But you should configure at least one authentication/authorization server and one accounting server, and at the same time, you should keep the RADIUS service port settings on the switch consistent with those on the RADIUS servers.



Actually, the RADIUS protocol configuration only defines the parameters used for information exchange between the switch and the RADIUS servers. To make these parameters take effect, you must reference the RADIUS scheme configured with these parameters in an ISP domain view. For specific configuration commands, refer to "AAA Configuration" on page 518.

Creating a RADIUS Scheme

The RADIUS protocol configuration is performed on a RADIUS scheme basis. You should first create a RADIUS scheme and enter its view before performing other RADIUS protocol configurations.

Table 407 Create a RADIUS scheme

Operation	Command	Description
Enter system view	**system-view**	-
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.



CAUTION: *A RADIUS scheme can be referenced by multiple ISP domains simultaneously.*

Configuring RADIUS Authentication/Authorization Servers

Table 408 Configure RADIUS authentication/authorization server

Operation	Command	Description
Enter system view	**system-view**	-
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.
Set the IP address and port number of the primary RADIUS authentication/authorization server	**primary authentication** *ip-address* [*port-number*]	Required By default, the IP address and UDP port number of the primary server are 0.0.0.0 and 1812 respectively.

Table 408 Configure RADIUS authentication/authorization server

Operation	Command	Description
Set the IP address and port number of the secondary RADIUS authentication/authorization server	**secondary authentication** *ip-address* [*port-number*]	Optional By default, the IP address and UDP port number of the secondary server are 0.0.0.0 and 1812 respectively.

CAUTION:

- *The authentication response sent from the RADIUS server to the RADIUS client carries the authorization information. Therefore, no separate authorization server can be specified.*
- *In an actual network environment, you can either specify two RADIUS servers as the primary and secondary authentication/authorization servers respectively, or specify only one server as both the primary and secondary authentication/authorization servers.*
- *The IP address and port number of the primary authentication server used by the default RADIUS scheme "system" are 127.0.0.1 and 1645.*

Configuring RADIUS Accounting Servers

Table 409 Configure RADIUS accounting server

Operation	Command	Description
Enter system view	**system-view**	-
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.
Set the IP address and port number of the primary RADIUS accounting server	**primary accounting** *ip-address* [*port-number*]	Required By default, the IP address and UDP port number of the primary accounting server are 0.0.0.0 and 1813.
Set the IP address and port number of the secondary RADIUS accounting server	**secondary accounting** *ip-address* [*port-number*]	Optional By default, the IP address and UDP port number of the secondary accounting server are 0.0.0.0 and 1813.
Enable stop-accounting packet buffering	**stop-accounting-buffer enable**	Optional By default, stop-accounting packet buffering is enabled.
Set the maximum number of transmission attempts of the buffered stop-accounting packets.	**retry stop-accounting** *retry-times*	Optional By default, the system tries at most 500 times to transmit a buffered stop-accounting request.
Set the maximum number of real-time accounting request attempts	**retry realtime-accounting** *retry-times*	Optional By default, the maximum number of real-time accounting request attempts is 5. After that, the user connection is cut down.

CAUTION:

- *In an actual network environment, you can either specify two RADIUS servers as the primary and secondary accounting servers respectively, or specify only one server as both the primary and secondary accounting servers. In addition, because RADIUS adopts different UDP ports to transceive authentication/authorization packets and the accounting packets, you must set a port number for accounting different from that set for authentication/authorization.*
- *Stop-accounting requests are critical to billing and will eventually affect the charges of the users; they are important for both the users and the ISP. Therefore, the switch should do its best to transmit them to the RADIUS accounting server. If the RADIUS server does not respond to such a request, the switch should first buffer the request on itself, and then retransmit the request to the RADIUS accounting server until it gets a response, or the maximum number of transmission attempts is reached (in this case, it discards the request).*
- *You can set the maximum number of real-time accounting request attempts in the case that the accounting fails. If the switch makes all the allowed real-time accounting request attempts but fails to perform accounting, it cuts down the connection of the user.*
- *The IP address and the port number of the default primary accounting server "system" are 127.0.0.1 and 1646.*
- *Currently, RADIUS does not support the accounting of FTP users.*

Configuring Shared Keys for RADIUS Packets

The RADIUS client and server adopt MD5 algorithm to encrypt the RADIUS packets exchanged with each other. The two parties verify the validity of the exchanged packets by using the shared keys that have been set on them, and can accept and respond to the packets sent from each other only if both of them have the same shared keys.

Table 410 Configure shared keys for RADIUS packets

Operation	Command	Description
Enter system view	**system-view**	-
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.
Set a shared key for the RADIUS authentication/authorization packets	**key authentication** *string*	Required By default, no shared key is set.
Set a shared key for the RADIUS accounting packets	**key accounting** *string*	Required By default, no shared key is set.

CAUTION: *You must set the share keys separately for the authentication/authorization packets and the accounting packets if the authentication/authorization server and the accounting server are different devices and the shared keys on the two servers are also different.*

Configuring the Maximum Number of Transmission Attempts of RADIUS Requests

The communication in RADIUS is unreliable because this protocol adopts UDP packets to carry data. Therefore, it is necessary for the switch to retransmit a RADIUS request if it gets no response from the RADIUS server after the response timeout timer expires. If the maximum number of transmission attempts is reached and the switch still receives no answer, the switch considers that the request fails.

Table 411 Configure the maximum transmission attempts of RADIUS request

Operation	Command	Description
Enter system view	**system-view**	-
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.
Set the maximum number of transmission attempts of RADIUS requests	**retry** *retry-times*	Optional By default, the system tries three times to transmit a RADIUS request.

Configuring the Supported RADIUS Server Type

Table 412 Configure the supported RADIUS server type

Operation	Command	Description
Enter system view	**system-view**	-
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.
Specify the type of RADIUS server supported by the switch	**server-type** { **extended** | **standard** }	Optional By default, the switch supports the standard type of RADIUS server. The type of RADIUS server in the default RADIUS scheme "system" is **extended**.

Configuring the Status of RADIUS Servers

For the primary and secondary servers (authentication/authorization servers, or accounting servers) in a RADIUS scheme:

When the switch fails to communicate with the primary server due to some server trouble, the switch will actively exchange packets with the secondary server.

After the time the primary server keeps in the block state exceeds the time set with the **timer quiet** command, the switch will try to communicate with the primary server again when it receives a RADIUS request. If the primary server recovers, the switch immediately restores the communication with the primary server instead of communicating with the secondary server, and at the same time restores the status of the primary server to the active state while keeping the status of the secondary server unchanged.

When both the primary and secondary servers are in active or block state, the switch sends packets only to the primary server.

Table 413 Set the status of RADIUS servers

Operation	Command	Description
Enter system view	**system-view**	-
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.
Set the status of the primary RADIUS authentication/authorization server	**state primary authentication** { **block** | **active** }	Optional By default, all the RADIUS servers in a customized RADIUS scheme are in the **block** state.
Set the status of the primary RADIUS accounting server	**state primary accounting** { **block** | **active** }	
Set the status of the secondary RADIUS authentication/authorization server	**state secondary authentication** { **block** | **active** }	
Set the status of the secondary RADIUS accounting server	**state secondary accounting** { **block** | **active** }	

Configuring the Attributes for Data to be Sent to RADIUS Servers

Table 414 Configure the attributes for data to be sent to the RADIUS servers

Operation	Command	Description
Enter system view	**system-view**	-
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.
Set the format of the user names to be sent to RADIUS servers	**user-name-format** { **with-domain** | **without-domain** }	Optional By default, the user names sent from the switch to RADIUS servers carry ISP domain names.
Set the units of measure for data flows sent to RADIUS servers	**data-flow-format data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } **packet** { **giga-packet** | **kilo-packet** | **mega- packet** | **one-packet** }	Optional By default, in a RADIUS scheme, the unit of measure for data is byte and that for packets is one-packet.
Set the source IP address used by the switch to send RADIUS packets	RADIUS scheme view **nas-ip** *ip-address* System view **radius nas-ip** *ip-address*	Optional By default, no source IP address is specified; and the IP address of the outbound interface is used as the source IP address.

CAUTION:

- *Generally, the access users are named in the userid@isp-name format. Where, isp-name behind the @ character represents the ISP domain name, by which the device determines which ISP domain it should ascribe the user to. However, some old RADIUS servers cannot accept the user names that carry ISP domain names. In this case, it is necessary to remove the domain names carried in the user names before sending the user names to the RADIUS server. For this*

*reason, the **user-name-format** command is designed for you to specify whether or not ISP domain names are carried in the user names sent to the RADIUS server.*

- *For a RADIUS scheme, if you have specified that no ISP domain names are carried in the user names, you should not adopt this RADIUS scheme in more than one ISP domain. Otherwise, such errors may occur: the RADIUS server regards two different users having the same name but belonging to different ISP domains as the same user (because the usernames sent to it are the same).*
- *In the default RADIUS scheme "system", no ISP domain names are carried in the user names by default.*

Configuring a Local RADIUS Authentication Server

Table 415 Configure local RADIUS authentication server

Operation	Command	Description
Enter system view	**system-view**	-
Create a local RADIUS authentication server	**local-server nas-ip** *ip-address* [**key** *password*]	Required By default, a local RADIUS authentication server has already been created. Its NAS-IP is 127.0.0.1.

CAUTION:

- *When you use the local RADIUS authentication server function, the UDP port number for the authentication/authorization service must be 1645, the UDP port number for the accounting service is 1646, and the IP addresses of the servers must be set to the addresses of the switch.*
- *The packet encryption key set by the **local-server** command with the **key** password parameter must be identical with the authentication/authorization packet encryption key set by the **key authentication** command in RADIUS scheme view.*
- *The switch supports up to 16 local RADIUS authentication servers (including the default local RADIUS authentication server).*

Configuring the Timers of RADIUS Servers

If the switch gets no response from the RADIUS server after sending out a RADIUS request (authentication/authorization request or accounting request) and waiting for a period of time, it should retransmit the packet to ensure that the user can obtain the RADIUS service. This wait time is called response timeout time of RADIUS servers; and the timer in the switch system that is used to control this wait time is called the response timeout timer of RADIUS servers.

For the primary and secondary servers (authentication/authorization servers, or accounting servers) in a RADIUS scheme:

When the switch fails to communicate with the primary server due to some server trouble, the switch will actively exchange packets with the secondary server.

After the time the primary server keeps in the block state exceeds the time set with the **timer quiet** command, the switch will try to communicate with the primary server again when it has a RADIUS request. If the primary server recovers, the switch immediately restores the communication with the primary server

instead of communicating with the secondary server, and at the same time restores the primary server to the active state while keeping the state of the secondary server unchanged.

To charge the users in real time, you should set the interval of real-time accounting. After the setting, the switch sends the accounting information of online users to the RADIUS server at regular intervals.

Table 416 Set the timers of RADIUS server

Operation	Command	Description
Enter system view	**system-view**	-
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.
Set the response timeout time of RADIUS servers	**timer response-timeout** *seconds* **timer** *seconds*	Optional By default, the response timeout timer of RADIUS servers expires in three seconds.
Set the wait time for the primary server to restore the active state	**timer quiet** *minutes*	Optional By default, the primary server waits five minutes before restoring the active state.
Set the real-time accounting interval	**timer realtime-accounting** *minutes*	Optional By default, the real-time accounting interval is 12 minutes.

Configuring the User Re-Authentication upon Device Restart Function



The function applies to the environment where the RADIUS authentication/accounting server is CAMS.

In an environment with a CAMS server, if the switch reboots after an exclusive user (a user whose concurrent online number is set to 1 on the CAMS) gets authenticated and authorized and begins being charged, the switch will give a prompt that the user has already been online when the user re-logs in to the network before CAMS performs online user detection, and the user cannot get authenticated. In this case, the user can access the network again only after the CAMS administrator manually removes the online information of the user.

The user re-authentication upon device restart function is designed to resolve the above problem. After this function is enabled, every time the switch restarts:

1. The switch generates an Accounting-On packet, which mainly contains the following information: NAS-ID, NAS-IP address (source IP address), and session ID.
2. The switch sends the Accounting-On packet to CAMS at regular intervals.
3. Once the CAMS receives the Accounting-On packet, it sends a response to the switch. At the same time it finds and deletes the original online information of the users who access the network through the switch before the restart according to

the information contained in this packet (NAS-ID, NAS-IP address and session ID), and ends the accounting of the users based on the last accounting update packet.

4 Once the switch receives the response from the CAMS, it stops sending other Accounting-On packets.

5 If the switch does not receives any response from the CAMS after the number of the Accounting-On packets it has sent reaches the configured maximum number, it does not send any more Accounting-On packets.



The switch can automatically generate the main attributes (NAS-ID, NAS-IP address and session ID) in the Accounting-On packets. However, you can also manually configure the NAS-IP address with the ***nas-ip*** *command. If you choose to manually configure the attribute, be sure to configure an appropriate and legal IP address. If this attribute is not configured, the switch will automatically use the IP address of the VLAN interface as the NAS-IP address.*

Table 417 Enable the user re-authentication upon device restart function

Operation	Command	Description
Enter system view	**system-view**	-
Enter RADIUS scheme view	**radius scheme** *radius-scheme-name*	-
Enable the user re-authentication upon device restart function	**accounting-on enable** [**send** *times* | **interval** *interval*]	By default, this function is disabled, and the system can send at most 15 Accounting-On packets consecutively at intervals of three seconds.

HWTACACS Configuration

Creating a HWTACACS Scheme

HWTACACS protocol is configured scheme by scheme. Therefore, you must create a HWTACACS scheme and enter HWTACACS view before you perform other configuration tasks.

Table 418 Create a HWTACACS scheme

Operation	Command	Description
Enter system view	**system-view**	-
Create a HWTACACS scheme and enter HWTACACS view	**hwtacacs scheme** *hwtacacs-scheme-name*	Required By default, no HWTACACS scheme exists.



CAUTION: *The system supports up to 16 HWTACACS schemes. You can only delete the schemes that are not being used.*

Configuring HWTACACS Authentication Servers

Table 419 Configure HWTACACS authentication servers

Operation	Command	Description
Enter system view	**system-view**	-
Create a HWTACACS scheme and enter its view	**hwtacacs scheme** *hwtacacs-scheme-name*	Required By default, no HWTACACS scheme exists.

Table 419 Configure HWTACACS authentication servers

Operation	Command	Description
Set the IP address and port number of the primary TACACS authentication server	**primary authentication** *ip-address* [*port*]	Required By default, the IP address of the primary authentication server is 0.0.0.0, and the port number is 0.
Set the IP address and port number of the secondary TACACS authentication server	**secondary authentication** *ip-address* [*port*]	Required By default, the IP address of the secondary authentication server is 0.0.0.0, and the port number is 0.

CAUTION:

- *The primary and secondary authentication servers cannot use the same IP address. Otherwise, the system will prompt unsuccessful configuration.*
- *You can remove a server only when it is not used by any active TCP connection for sending authentication packets.*

Configuring HWTACACS Authorization Servers

Table 420 Configure TACACS authorization servers

Operation	Command	Description
Enter system view	**system-view**	-
Create a HWTACACS scheme and enter its view	**hwtacacs scheme** *hwtacacs-scheme-name*	Required By default, no HWTACACS scheme exists.
Set the IP address and port number of the primary TACACS authorization server	**primary authorization** *ip-address* [*port*]	Required By default, the IP address of the primary authorization server is 0.0.0.0, and the port number is 0.
Set the IP address and port number of the secondary TACACS authorization server	**secondary authorization** *ip-address* [*port*]	Required By default, the IP address of the secondary authorization server is 0.0.0.0, and the port number is 0.

CAUTION:

- *The primary and secondary authorization servers cannot use the same IP address. Otherwise, the system will prompt unsuccessful configuration.*
- *You can remove a server only when it is not used by any active TCP connection for sending authorization packets.*

Configuring HWTACACS Accounting Servers

Table 421 Configure HWTACACS accounting servers

Operation	Command	Description
Enter system view	**system-view**	-

Table 421 Configure HWTACACS accounting servers

Operation	Command	Description
Create a HWTACACS scheme and enter its view	**hwtacacs scheme** *hwtacacs-scheme-name*	Required By default, no HWTACACS scheme exists.
Set the IP address and port number of the primary TACACS accounting server	**primary accounting** *ip-address* [*port*]	Required By default, the IP address of the primary accounting server is 0.0.0.0, and the port number is 0.
Set the IP address and port number of the secondary TACACS accounting server	**secondary accounting** *ip-address* [*port*]	Required By default, the IP address of the secondary accounting server is 0.0.0.0, and the port number is 0.
Enable the stop-accounting packets retransmission function and set the maximum number of attempts	**retry stop-accounting** *retry-times*	Optional By default, the stop-accounting packets retransmission function is enabled and the system can transmit a stop-accounting request for 100 times.

CAUTION:

- *The primary and secondary accounting servers cannot use the same IP address. Otherwise, the system will prompt unsuccessful configuration.*
- *You can remove a server only when it is not used by any active TCP connection for sending accounting packets.*

Configuring Shared Keys for RADIUS Packets

When using a TACACS server as an AAA server, you can set a key to improve the communication security between the router and the TACACS server.

The TACACS client and server adopt MD5 algorithm to encrypt the exchanged HWTACACS packets. The two parties verify the validity of the exchanged packets by using the shared keys that have been set on them, and can accept and respond to the packets sent from each other only if both of them have the same shared keys.

Table 422 Configure shared keys for TACACS packets

Operation	Command	Description
Enter system view	**system-view**	-
Create a HWTACACS scheme and enter its view	**hwtacacs scheme** *hwtacacs-scheme-name*	Required By default, no HWTACACS scheme exists.
Set a shared key for the HWTACACS accounting/authentication/authorization packets	**key** { **accounting** | **authorization** | **authentication** } *string*	Required By default, the TACACS server does not have a key.

Configuring the Attributes for Data to be Sent to TACACS Servers

Table 423 Configure the attributes for data to be sent to TACACS servers

Operation	Command	Description
Enter system view	**system-view**	-
Create a HWTACACS scheme and enter its view	**hwtacacs scheme** *hwtacacs-scheme-name*	Required By default, no HWTACACS scheme exists.
Set the format of the user names to be sent to TACACS servers	**user-name-format** { **with-domain** | **without-domain** }	Optional By default, the user names sent from the switch to TACACS servers carry ISP domain names.
Set the units of measure for data flows sent to TACACS servers	**data-flow-format data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** }	Optional By default, in a TACACS scheme, the unit of measure for data is byte and that for packets is one-packet.
	data-flow-format packet { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** }	
Set the source IP address used by the switch to send HWTACACS packets	HWTACACS view **nas-ip** *ip-address*	Optional By default, no source IP address is specified; the IP address of the outbound interface is used as the source IP address.
	System view **hwtacacs nas-ip** *ip-address*	

CAUTION: *Generally, the access users are named in the userid@isp-name format. Where, isp-name behind the @ character represents the ISP domain name. If the TACACS server does not accept the user name carrying isp domain name, it is necessary to remove the domain name from the user names before they are sent to the TACACS server.*

Configuring the Timers of TACACS Servers

Table 424 Configure the timers of TACACS servers

Operation	Command	Description
Enter system view	**system-view**	-
Create a HWTACACS scheme and enter its view	**hwtacacs scheme** *hwtacacs-scheme-name*	Required By default, no HWTACACS scheme exists.
Set the response timeout time of TACACS servers	**timer response-timeout** *seconds*	Optional By default, the response timeout time is five seconds.
Set the wait time for the primary server to restore the active state	**timer quiet** *minutes*	Optional By default, the primary server waits five minutes before restoring the active state.
Set the real-time accounting interval	**timer realtime-accounting** *minutes*	Optional By default, the real-time accounting interval is 12 minutes.

CAUTION:

- *The setting of real-time accounting interval is indispensable to real-time accounting. After an interval value is set, the device transmits the accounting*

information of online users to the TACACS accounting server at intervals of this value. Even if the server does not respond, the device does not cut down the online user.

- *The interval must be a multiple of 3.*
- *The setting of real-time accounting interval somewhat depends on the performance of the device and the TACACS server: A shorter interval requires higher device performance.*

Displaying and Maintaining AAA & RADIUS & HWTACACS Information

After the above configurations, you can execute the **display** commands in any view to view the operation of AAA, RADIUS and HWTACACS and verify your configuration.

You can use the **reset** command in user view to clear the corresponding statistics.

Table 425 Display AAA information

Operation	Command	Description
Display the configuration information about one specific or all ISP domains	**display domain** [*isp-name*]	You can execute the **display** command in any view
Display the information about user connections	**display connection** [**access-type dot1x** | **domain** *domain-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **radius-scheme** *radius-scheme-name* | **vlan** *vlan-id* | **ucibindex** *ucib-index* | **user-name** *user-name*]	
Display the information about local users	**display local-user** [**domain** *isp-name* | **idle-cut** { **disable** | **enable** } | **vlan** *vlan-id* | **service-type** { **ftp** | **lan-access** | **ssh** | **telnet** | **terminal** } | **state** { **active** | **block** } | **user-name** *user-name*]	

Table 426 Display and maintain RADIUS protocol information

Operation	Command	Description
Display the statistics about local RADIUS authentication server	**display local-server statistics**	You can execute the **display** command in any view
Display the configuration information about one specific or all RADIUS schemes	**display radius** [*radius-scheme-name*]	
Display the statistics about RADIUS packets	**display radius statistics**	
Display the buffered no-response RADIUS stop-accounting request packets	**display stop-accounting-buffer** { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* }	

Table 426 Display and maintain RADIUS protocol information

Operation	Command	Description
Delete the buffered no-response stop-accounting request packets	**reset stop-accounting-buffer** { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* }	You can execute the **reset** command in user view
Clear the statistics about the RADIUS protocol	**reset radius statistics**	

Table 427 Display and maintain HWTACACS protocol information

Operation	Command	Description
Display the configuration or statistic information about one specific or all HWTACACS schemes	**display hwtacacs** [*hwtacacs-scheme-name* [**statistics**]]	You can execute the **display** command in any view
Display the buffered HWTACACS stop-accounting request packets that are not responded to	**display stop-accounting-buffer** { **hwtacacs-scheme** *hwtacacs-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* }	
Clear the statistics about the TACACS protocol	**reset hwtacacs statistics** { **accounting** | **authentication** | **authorization** | **all** }	You can execute the **reset** command in user view
Delete the buffered stop-accounting request packets that are not responded to	**reset stop-accounting-buffer** { **hwtacacs-scheme** *hwtacacs-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* }	

AAA & RADIUS & HWTACACS Configuration Example

Remote RADIUS Authentication of Telnet/SSH Users

The configuration procedure for the remote authentication of SSH users through RADIUS server is similar to that of Telnet users. The following description only takes the remote authentication of Telnet users as example.

Network requirements

In the network environment shown in Figure 133, you are required to configure the switch so that the Telnet users logging into the switch are authenticated by the RADIUS server.

- A RADIUS server with IP address 10.1.1.1 is connected to the switch. This server will be used as the authentication server.
- On the switch, set the shared key that is used to exchange packets with the authentication RADIUS server to "expert".

You can use a CAMS server as the RADIUS server. If you use a third-party RADIUS server, you can select standard or extended as the server type in the RADIUS scheme.

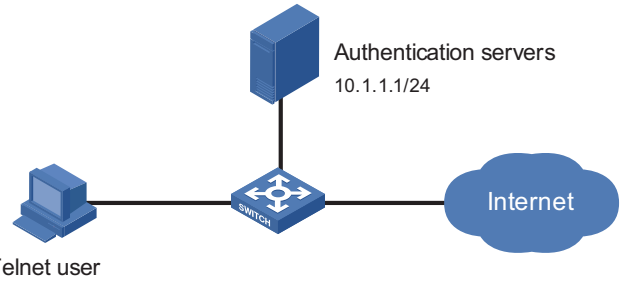
On the RADIUS server:

- Set the shared key it uses to exchange packets with the switch to "expert".
- Set the port number for authentication.
- Add Telnet user names and login passwords.

The Telnet user name added to the RADIUS server must be in the format of *userid@isp-name* if you have configure the switch to include domain names in the user names to be sent to the RADIUS server.

Network diagram

Figure 133 Remote RADIUS authentication of Telnet users



Configuration procedure

Enter system view.

```
<SW7750> system-view
[SW7750]
```

Adopt AAA authentication for Telnet users.

```
[SW7750] user-interface vty 0 4
[SW7750-ui-vty0-4] authentication-mode scheme
```

Configure an ISP domain.

```
[SW7750] domain cams
[SW7750-isp-cams] access-limit enable 10
[SW7750-isp-cams] quit
```

Configure a RADIUS scheme.

```
[SW7750] radius scheme cams
[SW7750-radius-cams] accounting optional
[SW7750-radius-cams] primary authentication 10.1.1.1 1812
```

```
[SW7750-radius-cams] key authentication expert
[SW7750-radius-cams] server-type Extended
[SW7750-radius-cams] user-name-format with-domain
[SW7750-radius-cams] quit
```

Associate the ISP domain with the RADIUS scheme.

```
[SW7750] domain cams
[SW7750-isp-cams] scheme radius-scheme cams
```

A Telnet user logging into the switch by a name in the format of *userid* @cams belongs to the cams domain and will be authenticated according to the configuration of the cams domain.

Local Authentication of FTP/Telnet Users

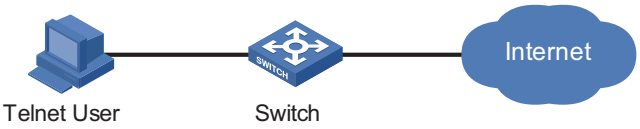
The configuration procedure for the local authentication of FTP users is similar to that of Telnet users. The following description only takes the local authentication of Telnet users as example.

Network requirements

In the network environment shown in Figure 134, you are required to configure the switch so that the Telnet users logging into the switch are authenticated locally.

Network diagram

Figure 134 Local authentication of Telnet users



Configuration procedure

Method 1: Using a local authentication scheme.

Enter system view.

```
<SW7750> system-view
[SW7750]
```

Adopt AAA authentication for Telnet users.

```
[SW7750] user-interface vty 0 4
[SW7750-ui-vty0-4] authentication-mode scheme
```

Create and configure a local user named telnet.

```
[SW7750] local-user telnet
[SW7750-luser-telnet] service-type telnet
[SW7750-luser-telnet] password simple extended
[SW7750-luser-telnet] attribute idle-cut 300 access-limit 5
```

```
[SW7750] domain system
[SW7750-isp-system] scheme local
```

A Telnet user logging into the switch with the name telnet@system belongs to the system domain and will be authenticated according to the configuration of the system domain.

Method 2: using a local RADIUS server

This method is similar to the remote authentication method described in "Remote RADIUS Authentication of Telnet/SSH Users" on page 537. You only need to change the server IP address, the authentication password, and the UDP port number for authentication service in configuration step "Configure a RADIUS scheme" in "Remote RADIUS Authentication of Telnet/SSH Users" on page 537 to 127.0.0.1, expert, and 1645 respectively, and configure local users (whether the name of local user carries domain name should be consistent with the configuration in RADIUS scheme).

TACACS Authentication, Authorization, and Accounting of Telnet Users

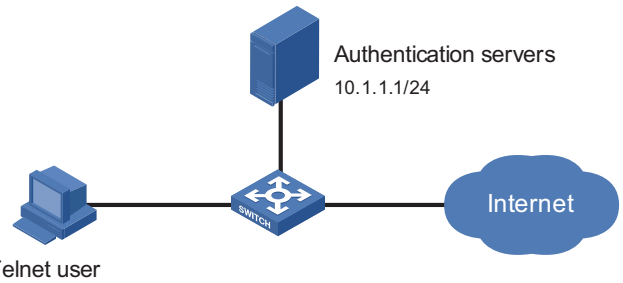
Network requirements

You are required to configure the switch so that the Telnet users logging in to the TACACS server are authenticated, authorized, and accounted. Configure the switch to A TACACS server with IP address 10.1.1.1 is connected to the switch. This server will be used as the AAA server. On the switch, set the shared key that is used to exchange packets with the AAA TACACS server to "expert". Configure the switch to strip off the domain name in the user name to be sent to the TACACS server.

Configure the shared key to "expert" on the TACACS server for exchanging packets with the switch.

Network diagram

Figure 135 Remote authentication and authorization of Telnet users



Configuration procedure

Add a Telnet user.

Omitted here

Configure a HWTACACS scheme.

```
<SW7750> system-view
[SW7750] hwtacacs scheme hwtac
[SW7750-hwtacacs-hwtac] primary accounting 10.1.1.1 49
```

```
[SW7750-hwtacacs-hwtac] primary authentication 10.1.1.1 49
[SW7750-hwtacacs-hwtac] primary authorization 10.1.1.1 49
[SW7750-hwtacacs-hwtac] key accounting expert
[SW7750-hwtacacs-hwtac] key authentication expert
[SW7750-hwtacacs-hwtac] key authorization expert
[SW7750-hwtacacs-hwtac] user-name-format without-domain
[SW7750-hwtacacs-hwtac] quit
```

Configure the domain name of the HWTACACS scheme to hwtac.

```
[SW7750] domain hwtacacs
[SW7750-isp-hwtacacs] scheme hwtacacs-scheme hwtac
```

Troubleshooting AAA & RADIUS & HWTACACS Configuration

Troubleshooting the RADIUS Protocol

The RADIUS protocol is at the application layer in the TCP/IP protocol suite. This protocol prescribes how the switch and the RADIUS server of the ISP exchange user information with each other.

Symptom 1: User authentication/authorization always fails.

Possible reasons and solutions:

- The user name is not in the userid@isp-name format, or no default ISP domain is specified on the switch - Use the correct user name format, or set a default ISP domain on the switch.
- The user is not configured in the database of the RADIUS server - Check the database of the RADIUS server, make sure that the configuration information about the user exists.
- The user input an incorrect password - Be sure to input the correct password.
- The switch and the RADIUS server have different shared keys - Compare the shared keys at the two ends, make sure they are identical.
- The switch cannot communicate with the RADIUS server (you can determine by pinging the RADIUS server from the switch) - Take measures to make the switch communicate with the RADIUS server normally.

Symptom 2: RADIUS packets cannot be sent to the RADIUS server.

Possible reasons and solutions:

- The communication links (physical/link layer) between the switch and the RADIUS server is disconnected/blocked - Take measures to make the links connected/unblocked.
- None or incorrect RADIUS server IP address is set on the switch - Be sure to set a correct RADIUS server IP address.
- One or all AAA UDP port settings are incorrect - Be sure to set the same UDP port numbers as those on the RADIUS server.

Symptom 3: The user passes the authentication and gets authorized, but the accounting information cannot be transmitted to the RADIUS server.

Possible reasons and solutions:

- The accounting port number is not properly set - Be sure to set a correct port number for RADIUS accounting.
- The switch requests that both the authentication/authorization server and the accounting server use the same device (with the same IP address), but in fact they are not resident on the same device - Be sure to configure the RADIUS servers on the switch according to the actual situation.

Troubleshooting the HWTACACS Protocol

See the previous section if you encounter an HWTACACS fault.

50 EAD CONFIGURATION

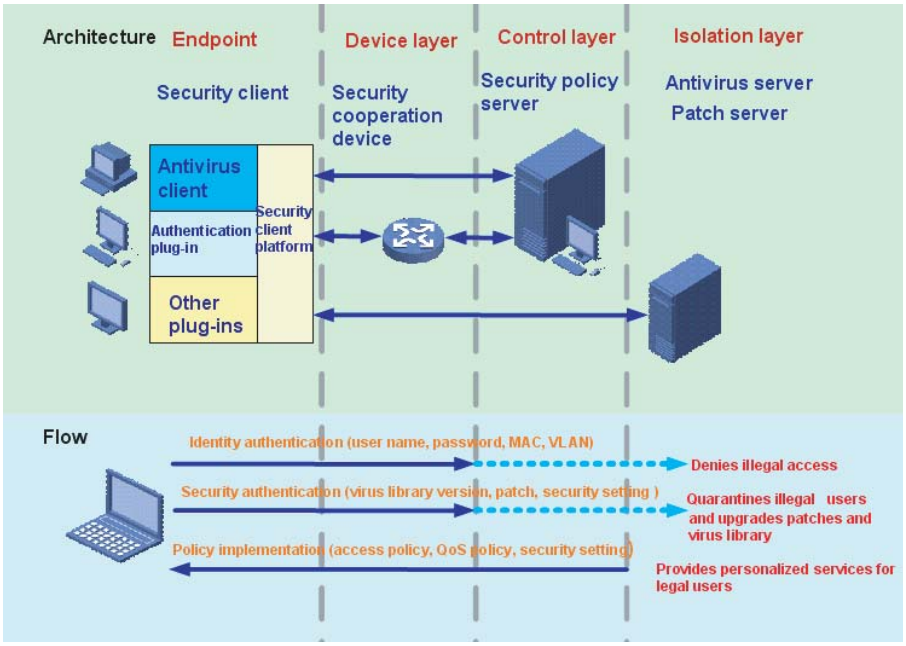
Introduction to EAD

Endpoint admission defense (EAD) is an attack defense solution that monitors endpoint admission. This enhances the active defense ability of endpoints, and prevents viruses and worms from spreading on the network. With the cooperation among security client, security policy server, access device, and antivirus software, EAD confines the endpoints that fail to comply with the security requirements to the quarantine area, thereby preventing hazardous terminals from compromising network security.

With EAD enabled, the switch determines the validity of session control packets it receives according to the source IP address of the packets. Only those session control packets sent from the authentication server and the security policy server can be regarded as valid.

Basic EAD functions are implemented through the cooperation among security client, security cooperation device (switch), security policy server, antivirus server, and patch server, as shown in Figure 136.

Figure 136 EAD basic principle

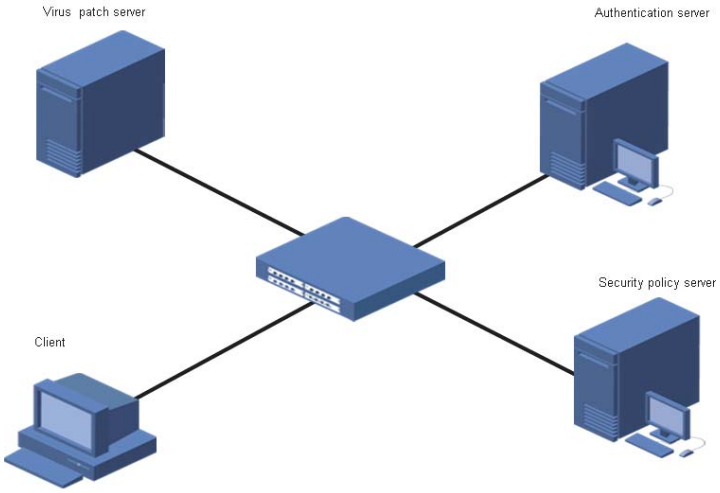


Typical Network Application of EAD

The EAD scheme checks the security status of the user, and implements the user access control policy forcibly according to the result. Therefore, those non-compliant users are isolated and are forced to upgrade virus database

software and install system patches. Figure 137 shows the typical network application of EAD.

Figure 137 Typical network application of EAD



The security client (software installed on PC) checks the security status of a client that just passes the authentication, and interacts with the security policy server. If the client is not compliant with the security standard, the security policy server issues ACL control packets to the switch to control which addresses the client can access.

After the client is patched and compliant with the required security standard, the security policy server reissues an ACL to the switch to assign the access right to the client.

EAD Configuration

Configuration prerequisites

EAD is implemented typically in RADIUS scheme. Before configuring EAD, perform the following configuration:

- Configuring the attributes, such as the user name, user type, and password for access users. If local authentication is performed, you need to configure these attributes on the switch; if remote authentication is performed, you need to configure these attributes on AAA sever.
- Configuring RADIUS scheme.
- Associating domain with RADIUS scheme.

For the detailed configuration procedure, refer to "AAA & RADIUS & HWTACACS Configuration" on page 507.

Configuring EAD

Table 428 EAD configuration

Operation	Command	Description
Enter system view	**system-view**	-

Table 428 EAD configuration

Operation	Command	Description
Enter RADIUS scheme view	**radius scheme** *radius-scheme-name*	-
Configure the RADIUS server type to **extended**	**server-type extended**	Optional By default, for a new RADIUS scheme, the server type is **standard**; The type of RADIUS server in the default RADIUS scheme "system" is **extended**.
Configure the IP address for the security policy server	**security-policy-server** *ip-address*	Optional This configuration is optional if the security policy server and RADIUS server run on the same machine; otherwise, it is required.

EAD Configuration Example

Network requirements

In Figure 138:

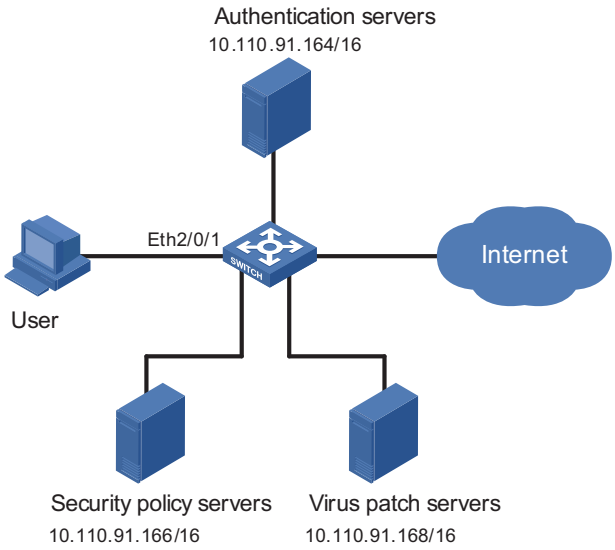
- A user is connected to Ethernet2/0/1 of the switch
- The user adopts 802.1X client supporting EAD extended function
- By configuring the switch, user remote authentication is implemented through RADIUS server and EAD control is achieved through security policy server.

The following are the configuration tasks:

- Connect the RADIUS authentication server to the switch. The IP address of the server is 10.110.91.164, and the switch adopts the port with port number 1812 to communicate with the authentication server.
- Configure the authentication server type to **extended**.
- Configure the encryption password for exchanging messages between the switch and RADIUS server to "expert".
- Configure the IP address of the security policy server to 10.110.91.166.

Network diagram

Figure 138 EAD configuration example



Configuration procedure

Configure 802.1X on the switch. Refer to the “802.1x Configuration” on page 399 for detailed description.

Configure domain.

```
<SW7750> system-view
[SW7750] domain system
[SW7750-isp-system] quit
```

Configure RADIUS scheme.

```
[SW7750] radius scheme cams
[SW7750-radius-cams] primary authentication 10.110.91.164 1812
[SW7750-radius-cams] key authentication expert
[SW7750-radius-cams] accouting optional
[SW7750-radius-cams] server-type extended
```

Configure the IP address for the security policy server.

```
[SW7750-radius-cams] security-policy-server 10.110.91.166
```

Associate domain with RADIUS scheme.

```
[SW7750-radius-cams] quit
[SW7750] domain system
[SW7750-isp-system] radius-scheme cams
```

51 TRAFFIC ACCOUNTING CONFIGURATION

The traffic accounting module mentioned in this chapter refers to LS81VSNP I/O Module (line processing unit).

Introduction to Traffic Accounting

Some accounting servers, such as CAMS, can perform accounting for successfully authenticated 802.1x users based on time or traffic. Traffic accounting enables the switch where the users are authenticated to account for the traffic generated when the users are online and send traffic accounting results to the accounting server to charge the online users.

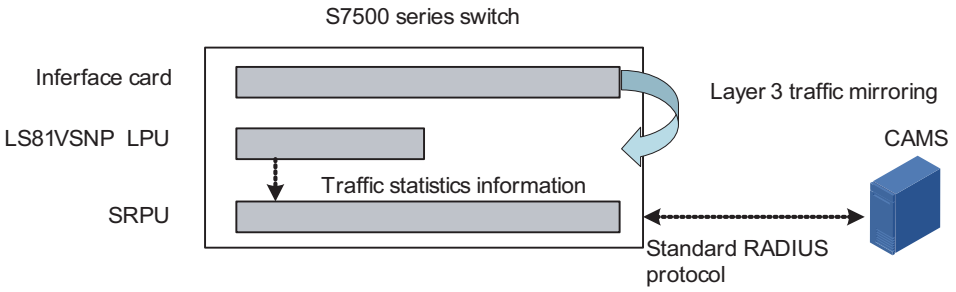
Related Concepts of Traffic Accounting

- Traffic group: a mechanism used to classify destination networks by accounting attributes. The accounting attributes of a traffic group include whether or not to charge and the charge rate.
- Traffic group accounting address: a network IP address configured for a traffic group. You can configure some network addresses for a traffic group, and then traffic generated by accessing these addresses will be accounted.
- Traffic collection module: an interface module configured to perform traffic collection. A traffic collection module sends all the traffic passing through it to the traffic accounting module.
- Traffic accounting module: the module which performs traffic analysis, calculation and statistics.
- Traffic collection: the process of sending the traffic passing through the traffic collection module to the traffic accounting module.
- Traffic accounting: the process that the traffic accounting module follows to analyze and calculate the traffic obtained from the traffic collection module. Traffic accounting is performed based on the users' online IP addresses and the traffic groups to which the accessed networks belong.

Implementation Process of Traffic Accounting

Figure 139 shows the implementation process of traffic accounting on the 3Com Switch 7750s.

Figure 139 Implementation process of traffic accounting



The following details the traffic accounting procedure:

1. After a user passes the 802.1x authentication, the user goes online successfully.
2. The authenticator device acquires the online IP address of the user and starts to account for the traffic of the user.
3. The user accesses networks and traffic is generated.
4. The traffic collection module sends the user's online traffic to the traffic accounting module (LS81VSNP I/O Module).
5. The traffic accounting module performs traffic statistics based on traffic group, and generates traffic accounting statistics, which reflects the accumulated amount of the traffic generated since the user gets online.
6. The traffic accounting module periodically sends update traffic accounting statistics to the accounting server.
7. When the user goes offline, the authenticator device sends the total traffic amount to the accounting server.
8. The accounting process is over for this user.

Configuring Traffic Accounting

Prerequisites

- A service module that can be used as the traffic accounting module is plugged into the switch.
- 802.1x is enabled on the switch.
- A CAMS server is properly configured.

This article introduces the configuration of traffic accounting. The configuration of 802.1x and CAMS server is not covered here.

Configuring Traffic Accounting

The following table describes the configuration tasks for traffic accounting.

Table 429 Configure the traffic accounting function

Operation	Command	Description
Enter system view	**system-view**	-

Table 429 Configure the traffic accounting function

Operation	Command	Description
Configure the traffic accounting slot	**traffic-accounting accounting-slot** *slot-num*	Required ■ The traffic accounting slot you specified must be the slot where the traffic accounting module resides. ■ You will enter the traffic accounting view directly after the configuration succeeds. ■ By default, no traffic accounting slot is specified.
Specify a traffic collection card	**Traffic-slot** *slot-num*	Required
Enable the traffic accounting function	**accounting enable**	Required By default, this function is disabled on the traffic accounting module.

Table 430 Configure traffic group

Configuration	Command	Description
Enter system view	**system-view**	-
Create a traffic group and enter traffic group view	**traffic-accounting traffic-group** *group-name*	Required
Configure a network address for the traffic group	**network** *ip-address* { *mask* | *mask-len* }	Required

Table 431 Configure a traffic group for a domain

Configuration	Command	Description
Enter system view	**system-view**	-
Enter ISP domain view	**domain** *domain-name*	-
Set the accounting mode to traffic accounting	**accounting-mode traffic**	Required By default, the system performs accounting based on time.
Configure the domain to use a specified traffic group	**traffic-group** *group-name* **rate** *idnum*	Required



- *The interface module that connects external networks (Internet) should be configured as traffic collection modules.*
- *Currently, only single rate is supported, and multi-rate is not supported.*

Displaying Traffic Accounting

After the above configuration, you can execute the **display** command in any view to display the operation status of traffic accounting and verify your configuration.

Table 432 Display traffic accounting

Operation	Command	Description
Display traffic group information	**display traffic-accounting traffic-group** [*group-name*]	You can execute the **display** command in any view.
Display traffic accounting configuration	**display traffic-accounting accounting-slot** [*slot-num*]	
Display traffic accounting statistics of one or all online users	**display traffic-accounting statistics** [*ip-address*]	

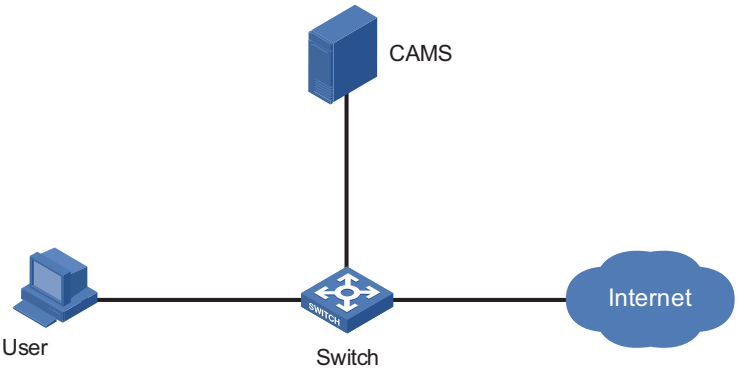
Traffic Accounting Configuration Example

Network requirements

- A user running 802.1x authentication client accesses the Internet through a switch. The user can access external networks after passing the authentication. The accounting mode is traffic accounting. When the user accesses the networks 11.127.1.0/24 and 12.127.1.0/24, the accounting server CAMS charges the user according to the user's online traffic. When the user accesses other networks, however, the user is not charged.

Network diagram

Figure 140 Network diagram for traffic accounting



Configuration procedure

Configure a traffic accounting group named somegroup.

```
<SW7750> system-view
[SW7750] traffic-accounting traffic-group somegroup
```

Configure the following two destination network IP addresses for the traffic accounting group.

```
[SW7750-traffic-group-somegroup] network 11.127.1.0 24
[SW7750-traffic-group-somegroup] network 12.127.1.0 24
[SW7750-traffic-group-somegroup] quit
```

Enter the user's domain view (suppose the user belongs to domain aaa), set the accounting mode to traffic accounting and configure the domain to use the traffic group.

```
[SW7750] domain aaa
[SW7750-isp-aaa] accounting-mode traffic
```

```
[SW7750-isp-aaa] traffic-group somegroup rate 1
[SW7750-isp-aaa] quit
```

Configure the traffic accounting module, specify the traffic collection module, and enable the traffic accounting function.

```
[SW7750] traffic-accounting accounting-slot 2
[SW7750-accounting-slot-2] traffic-slot 3
[SW7750-accounting-slot-2] accounting enable
```

52 VRRP CONFIGURATION

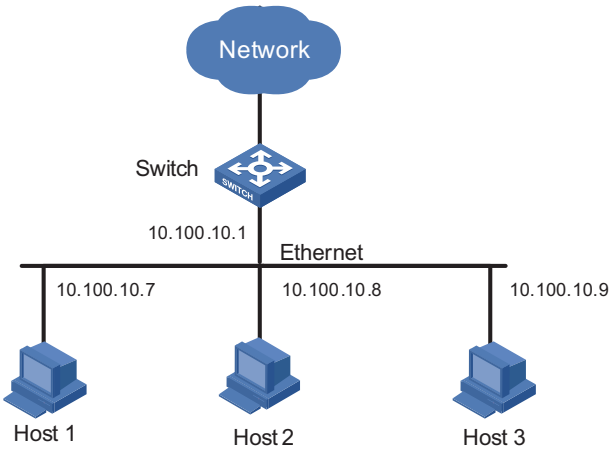
VRRP Overview

Virtual router redundancy protocol (VRRP) is a fault-tolerant protocol.

As shown in Figure 141, in general,

- A default route (for example, the next hop address of the default route is 10.100.10.1, as shown in the following figure) is configured for every host on a network.
- The packets destined to the external network segments and sourced from these hosts go through the default routes to the Layer 3 Switch, implementing communication between these hosts and the external network.
- If Switch fails, all the hosts on this segment taking Switch as the next-hop through the default routes are cut off from the external network.

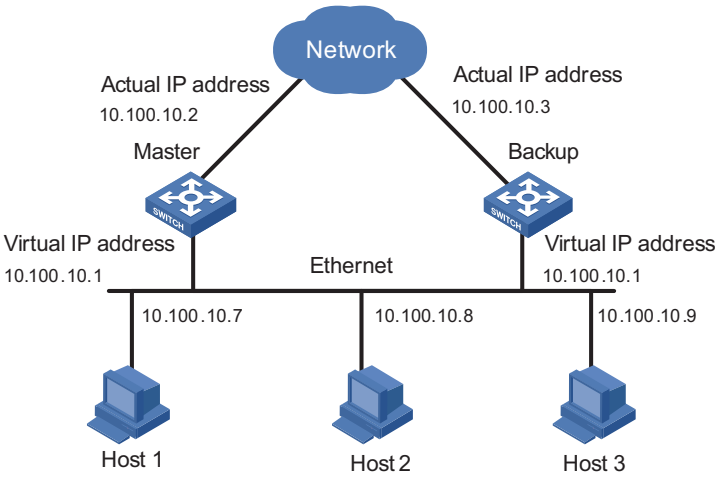
Figure 141 LAN Networking



VRRP, designed for LANs with multicast and broadcast capabilities (such as Ethernet), settles the problem caused by switch failures.

VRRP combines a group of LAN switches, including a master switch and several backup switches, into a virtual router, or a backup group.

Figure 142 Virtual router



The switches in a backup group have the following features:

- This virtual router has its own IP address: 10.100.10.1 (which can be the interface address of a switch within the backup group).
- The switches within the backup group have their own IP addresses (such as 10.100.10.2 for the master switch and 10.100.10.3 for the backup switch).
- Hosts on the LAN only know the IP address of this virtual router, that is, 10.100.10.1, but not the specific IP addresses 10.100.10.2 of the master switch and 10.100.10.3 of the backup switch.
- Hosts in the LAN use the IP address of the virtual router (that is, 10.100.10.1) as their default next-hop IP addresses.

Therefore, hosts within the network will communicate with the other networks through this virtual router.

If the master switch in the backup group goes down, the backup switch with the highest priority functions as the new master switch to guarantee normal communication between the hosts and the external networks. This ensures the communications between the hosts and the external networks.

Virtual Router Overview

After you enable VRRP on the switches of a backup group, a virtual router is formed. You can perform related configuration on the virtual router.

Configuring a virtual router IP address

The IP address of the virtual router can be an unassigned IP address of the network segment where the backup group is located or the interface IP address of a member switch in the backup group. Virtual router IP address has the following features:

- You can specify the virtual router IP address as the IP address used by a member switch in the backup group. In this case, the switch is called an IP address owner.
- A backup group is established if it is assigned an IP address for the first time. If you then add other IP addresses to the backup group, the IP addresses are added to the virtual router IP address list of the backup group.

- The virtual router IP address and the IP addresses used by the member switches in a backup group must belong to the same network segment. If not, the backup group will be in the initial state (the state before you configure the VRRP on the switches of the group). In this case, VRRP does not take effect.
- A backup group is removed if all its virtual router IP addresses are removed. In this case, all the configurations performed for the backup group get ruined.

According to the standard VRRP, an attempt to ping the IP address of a virtual router will result in failure. Thus, you cannot locate the network fault by using the **ping** command.

To solve this problem, you can enable the switches in a backup group to respond the **ping** operations destined for the virtual router IP addresses.

Mapping Virtual IP Addresses to MAC Addresses

A Switch 7750 provides the following functions in addition to forwarding data correctly.

- You can map multiple virtual IP addresses of the backup group to a virtual MAC address as needed. You can also map virtual IP addresses to the MAC address of a switch routing interface.
- You need to map the IP addresses of the backup group to the MAC addresses before enabling VRRP feature on a Switch 7750. If VRRP is already enabled, the system does not support this configuration.

By default, virtual router IP addresses are mapped to the virtual MAC address of a backup group.



When you map a virtual IP address to the virtual MAC address on a Switch 7750, the number of backup groups that can be configured on a VLAN interface is determined by the chips used. Refer to device specification for detail.

Backup Group Configuration Tasks

Configuring switch priority

You can configure the priority of a switch in a backup group. VRRP will determine the status of each switch in a backup group according to the priority of the switch. The master switch in a backup group is the one currently with the highest priority.

Switch priority ranges from 0 to 255 (a larger number indicates a higher switch priority) and defaults to 100. Note that only 1 through 254 are available to users. Switch priority of 255 is reserved for IP address owners.



The priority of the IP address owner is fixed to 255.

Configuring preemptive mode for a switch in a backup group

As long as a switch in the backup group becomes the master switch, other switches, even if they are configured with a higher priority later, do not preempt the master switch unless they operate in preemptive mode. The switch operating in preemptive mode will become the master switch when it finds its priority is higher than that of the current master switch, and the former master switch becomes a backup switch accordingly.

You can configure a Switch 7750 to operate in preemptive mode. You can also set the delay period. A backup switch waits for a period of time (the delay period) before becoming a master switch. Setting a delay period aims at:

In an unstable network, backup switches in a backup group possibly cannot receive packets from the master in time due to network congestions even if the master operates properly. This causes the master of the backup group being determined frequently. With the configuration of delay period, the backup switch will wait for a while if it does not receive packets from the master switch in time. A new master is determined only after the backup switches do not receive packets from the master switch after the specified delay time.

Configuring authentication type and authentication key for a switch in a backup group

VRRP provides following authentication types:

- **simple**: Simple character authentication
- **md5**: MD5 authentication

In a network under possible security threat, the authentication type can be set to **simple**. Then the switch adds the authentication key into the VRRP packets before transmitting them. The receiver will compare the authentication key of the packet with the locally configured one. If they are the same, the packet will be taken as a true and legal one. Otherwise it will be regarded as an illegal packet and be discarded. In this case, a simple authentication key should not exceed eight characters.

In a vulnerable network, the authentication type can be set to **md5**. The switch then uses the authentication type provided by the Authentication Header, and MD5 algorithm to authenticate the VRRP packets. In this case, you need to set an authentication key in plain text comprising up to eight characters or an authentication key of a 24-character encrypted string.

Packets that fail to pass the authentication are discarded. The switch then sends trap packets to the network management system.

Configuring VRRP timer

The master switch advertises its normal operation state to the switches within the VRRP backup group by sending VRRP packets once in each specified interval (determined by the *adver-interval* argument). If the backup switches do not receive VRRP packets from the master after a specific period (determined by the *master-down-interval* argument), they consider the master is down and initiates the process to determine the master switch.

You can adjust the frequency in which a master sends VRRP packets by setting the corresponding VRRP timers (that is, the *adver-interval* argument). The *master-down-interval* argument is usually three times of the *adver-interval* argument. Excessive network traffic or differences between the timers of different switches will result in *master-down-interval* timing out and state changing abnormally. Such problems can be solved through prolonging the *adver-interval* and setting delay time. If you configure the preemption delay for a backup switch, the switch preempts the master after the period specified by the preemption delay

if it does not receive a VRRP packet from the master for the period specified by the *master-down-interval* argument.

Configuring the VLAN interfaces/Ethernet ports to be tracked for a backup group

The VLAN interface/Ethernet port tracking function expands the backup group function. With this function enabled, the backup group function is provided not only when the interface where the backup group resides fails, but also when other interfaces/Ethernet ports are unavailable. By executing the related command you can track an interface/Ethernet port.

When a tracked VLAN interface goes down, the priority of the switch owning the interface will reduce automatically by a specified value (the *value-reduced* argument). If the switches with their priorities higher than that of the current master switch exist in the backup group, a new master switch will be then determined.

Similarly, when the tracked Ethernet port is down, the priority of its switch will be degraded by *value-reduced* automatically. As a result, other switch in the backup group may have a higher priority than this switch and therefore take over the role as a master switch.

- *The Ethernet port tracked can be in or out of the VLAN in whose interface the backup group resides.*
- *If a switch is the IP address owner, the VLAN interface/Ethernet port tracking function can not be enabled for the switch.*
- *If a tracked VLAN interface/Ethernet port goes down, when it is up again, the priority of the corresponding switch is automatically restored.*
- *Each backup group can track up to eight VLAN interfaces/Ethernet ports.*

VRRP Configuration

Introduction to VRRP Configuration Tasks

Table 433 VRRP configuration tasks

Configuration	Description	Related section
Configure a virtual router IP address	Required	"Configuring a Virtual Router IP address" on page 557
Configure backup group-related parameters	Required	"Configuring Backup Group-Related Parameters" on page 558

Configuring a Virtual Router IP address

Table 434 lists the operations to configure a virtual router IP address (suppose you have correctly configured the mapping between the port and VLAN):

Table 434 Configure a virtual router IP address

Operation	Command	Description
Enter system view	**system-view**	-

Table 434 Configure a virtual router IP address

Operation	Command	Description
Configure that the virtual IP address can be pinged	**vrrp ping-enable**	Optional By default, the virtual IP address cannot be pinged.
Map the virtual router IP address to a MAC address	**vrrp method** { **real-mac** | **virtual-mac** }	Optional By default, the virtual IP address of a backup group is mapped to a virtual router IP address.
Create a VLAN	**vlan** *vlan-id*	- This operation creates the VLAN to which the backup group corresponds. The *vlan-id* argument is the ID of the VLAN.
Quit to system view	**quit**	-
Enter VLAN interface view	**interface Vlan-interface** *vlan-id*	-
Configure a virtual router IP address	**vrrp vrid** *virtual-router-id* **virtual-ip** *virtual-address*	Optional By default, no IP address is configured for the virtual router.

Configuring Backup Group-Related Parameters

Table 435 lists the operations to configure a switch in a backup group.

Table 435 Configure backup group-related parameters

Operation	Command	Description
Enter system view	**system-view**	-
Create a VLAN	**vlan** *vlan-id*	-
Quit to system view	**quit**	-
Enter VLAN interface view	**interface Vlan-interface** *valn-id*	-
Configure the priority of the backup group	**vrrp vrid** *virtual-router-id* **priority** *priority*	Optional By default, the priority of a backup group is 100.
Configure the preemptive mode and delay period for the backup group	**vrrp vrid** *virtual-router-id* **preempt-mode** [**timer delay** *delay-value*]	Optional By default, a backup group operates in the preemptive mode.
Configure the authentication type and authentication key	**vrrp vrid** *virtual-router-id* **authentication-mode** *authentication-type authentication-key*	Optional By default, a backup group does not authenticate.
Configure the VRRP timer	**vrrp vrid** *virtual-router-id* **timer advertise** *adver-interval*	Optional By default, the interval for the master switch in a backup group to send VRRP packets is 1 second.
Specify the interface/Ethernet port to be tracked	**vrrp vrid** *virtual-router-id* **track interface** *interface-type interface-number* [**reduced** *value-reduced*]	Optional *value-reduced*: Value by which the priority is to be reduced. By default, this value is 10.

Displaying and Maintaining VRRP

After the above configuration, you can execute the **display** command in any view to view VRRP configuration and verify the configuration effect. And in user view, you can execute the **reset** command to clear the VRRP statistics and execute the **debugging** command to debug the VRRP.

Table 436 Display and Maintain VRRP

Operation	Command	Description
Display the VRRP statistics information	**display vrrp statistics** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]	You can execute the **display** command in any view.
Display the VRRP status information	**display vrrp** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]	
Display the detailed VRRP information	**display vrrp verbose** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]	
Clear the VRRP statistics information	**reset vrrp statistics** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]	You can execute the **reset** command in user view.

VRRP Configuration Example

Single-VRRP Backup Group Configuration

Network requirements

Host A uses the VRRP virtual router comprising switch A and switch B as its default gateway to visit host B on the Internet.

The information about the VRRP backup group is as follows:

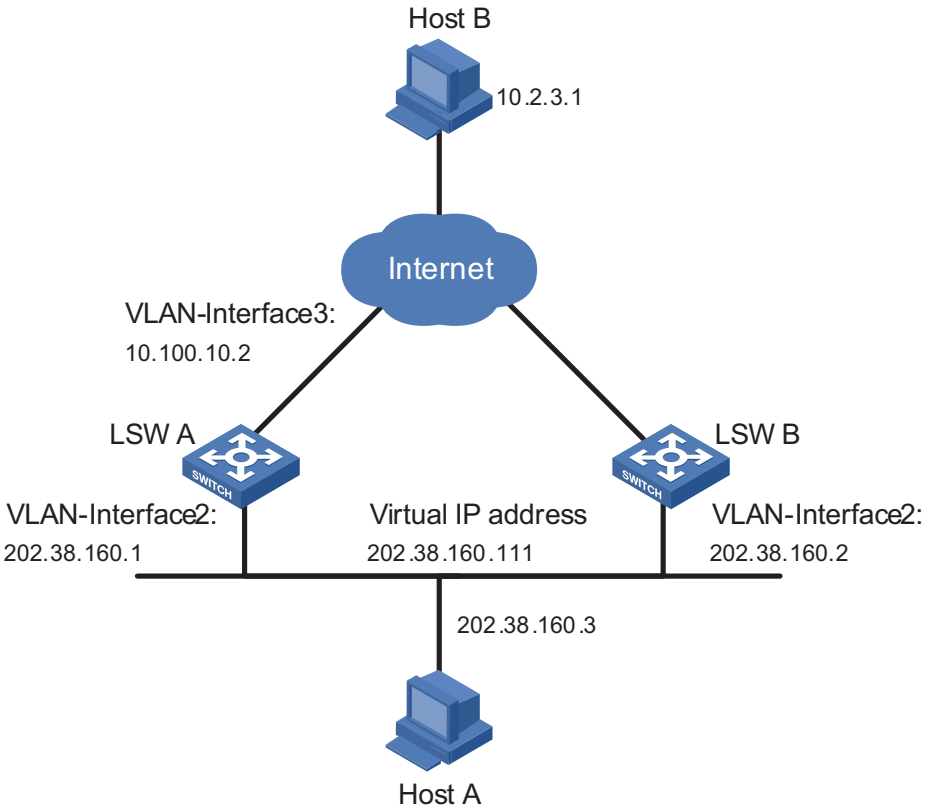
- VRRP backup group ID: 1
- Virtual router IP address: 202.38.160.111
- Master switch: Switch A
- Backup switch: Switch B
- Preemptive mode: enabled

Table 437 Network description

Switch	Ethernet port connecting to Host A	IP address of the VLAN interface	Switch priority in the backup group	Preemptive mode
LSW-A	Ethernet 1/0/6	202.38.160.1/24	110	Enabled
LSW-B	Ethernet 1/0/5	202.38.160.2/24	100 (default)	Enabled

Network diagram

Figure 143 Network diagram for single-VRRP backup group configuration



Configuration procedure

- Configure Switch A.

Configure VLAN 2.

```
<LSW-A> system-view
[LSW-A] vlan 2
[LSW-A-vlan2] port Ethernet 1/0/6
[LSW-A-vlan2] quit
[LSW-A] interface Vlan-interface 2
[LSW-A-Vlan-interface2] ip address 202.38.160.1 255.255.255.0
[LSW-A-Vlan-interface2] quit
```

Enable a backup group to respond to ping operations destined for its virtual router IP address.

```
[LSW-A] vrrp ping-enable
```

Create a backup group.

```
[LSW-A] interface Vlan-interface 2
[LSW-A-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
```

Set the priority for the backup group.

```
[LSW-A-Vlan-interface2] vrrp vrid 1 priority 110
```

Configure the preemptive mode for the backup group.

```
[LSW-A-Vlan-interface2] vrrp vrid 1 preempt-mode
```

- Configure Switch B.

Configure VLAN 2.

```
<LSW-B> system-view
[LSW-B] vlan 2
[LSW-B-Vlan2] port Ethernet 1/0/5
[LSW-B-vlan2] quit
[LSW-B] interface Vlan-interface 2
[LSW-B-Vlan-interface2] ip address 202.38.160.2 255.255.255.0
[LSW-B-Vlan-interface2] quit
```

Enable a backup group to respond to ping operations destined for its virtual router IP address.

```
[LSW-B] vrrp ping-enable
```

Create a backup group.

```
[LSW-B] interface Vlan-interface 2
[LSW-B-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
```

Configure the preemptive mode for the backup group.

```
[LSW-B-Vlan-interface2] vrrp vrid 1 preempt-mode
```

The IP address of the default gateway of Host A can be configured to be 202.38.160.111.

Normally, Switch A functions as the gateway, but when Switch A is turned off or malfunctions, Switch B will function as the gateway instead.

Configure Switch A to operate in preemptive mode, so that it can resume its gateway function as the master switch after recovery.

VRRP Tracking Interface Configuration

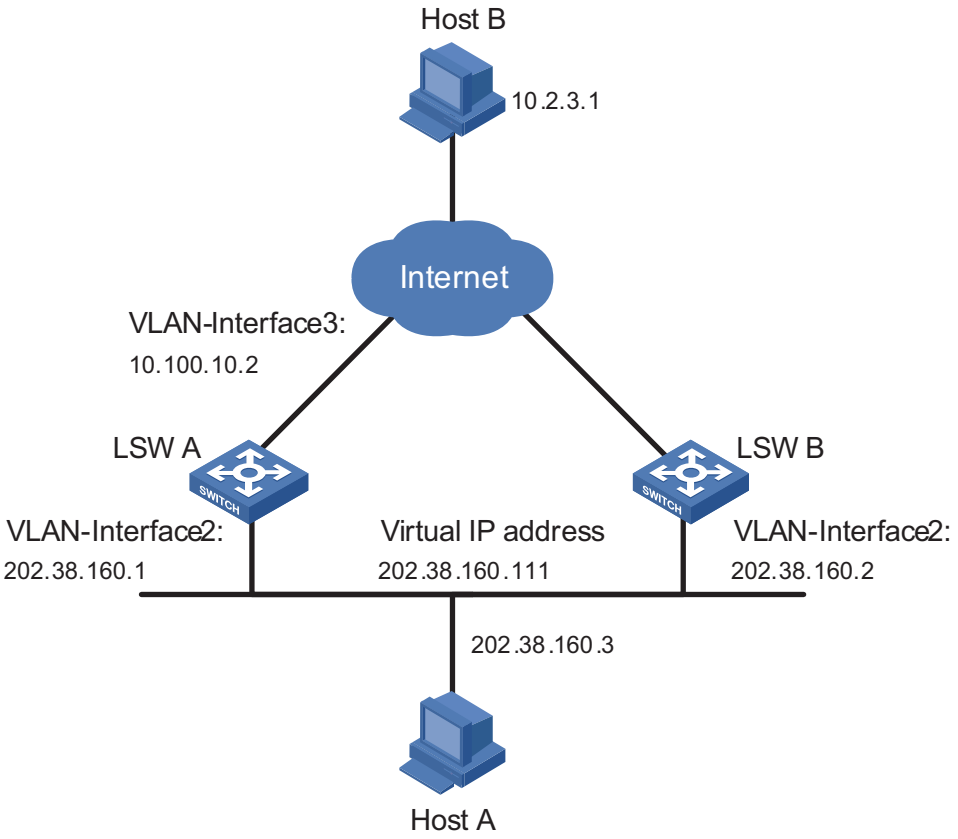
Network requirements

Even when Switch A is still functioning, Switch B (with another link to connect with the outside) can function as a gateway when the interface on Switch A and connecting to Internet does not function properly. This can be implemented by enabling the VLAN interface tracking function.

The VRRP backup group ID is set to 1, with configurations of authorization key and timer.

Network diagram

Figure 144 Network diagram for interface tracking configuration



Configuration procedure

- Configure Switch A.

Configure VLAN 2.

```
<LSW-A> system-view
[LSW-A] vlan 2
[LSW-A-vlan2] port Ethernet 1/0/6
[LSW-A-vlan2] quit
[LSW-A] interface Vlan-interface 2
[LSW-A-Vlan-interface2] ip address 202.38.160.1 255.255.255.0
[LSW-A-Vlan-interface2] quit
```

Configure that the virtual router can be pinged.

```
[LSW-A] vrrp ping-enable
```

Create a backup group.

```
[LSW-A] interface Vlan-interface 2
[LSW-A-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
```

Set the priority for the backup group.

```
[LSW-A-Vlan-interface2] vrrp vrid 1 priority 110
```

Set the authentication type for the backup group to **md5,** and the password to abc123.

```
[LSW-A-Vlan-interface2] vrrp vrid 1 authentication-mode md5 abc123
```

Configure that the master switch to send VRRP packets once in every 5 seconds.

```
[LSW-A-Vlan-interface2] vrrp vrid 1 timer advertise 5
```

Set the tracked VLAN interface.

```
[LSW-A-Vlan-interface2] vrrp vrid 1 track interface Vlan-interface 3
 reduced 30
```

- Configure switch B.

Configure VLAN 2.

```
<LSW-B> system-view
[LSW-B] vlan 2
[LSW-B-vlan2] port Ethernet 1/0/5
[LSW-B-vlan2] quit
[LSW-B] interface Vlan-interface 2
[LSW-B-Vlan-interface2] ip address 202.38.160.2 255.255.255.0
[LSW-B-Vlan-interface2] quit
```

Configure that the virtual router can be pinged.

```
[LSW-B] vrrp ping-enable
```

Create a backup group.

```
[LSW-B] interface Vlan-interface 2
[LSW-B-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
```

Set the authentication key for the backup group.

```
[LSW-B-Vlan-interface2] vrrp vrid 1 authentication-mode md5 abc123
```

Set the master to send VRRP packets once in every 5 seconds.

```
[LSW-B-Vlan-interface2] vrrp vrid 1 timer advertise 5
```

Normally, Switch A functions as the gateway, but when VLAN 3 interface on Switch A goes down, its priority will be reduced by 30, lower than that of Switch B so that Switch B will preempt the master for gateway services instead.

When VLAN 3 interface recovers, switch A will resume its gateway function as the master.

Multiple-VRRP Backup Group Configuration

Network requirements

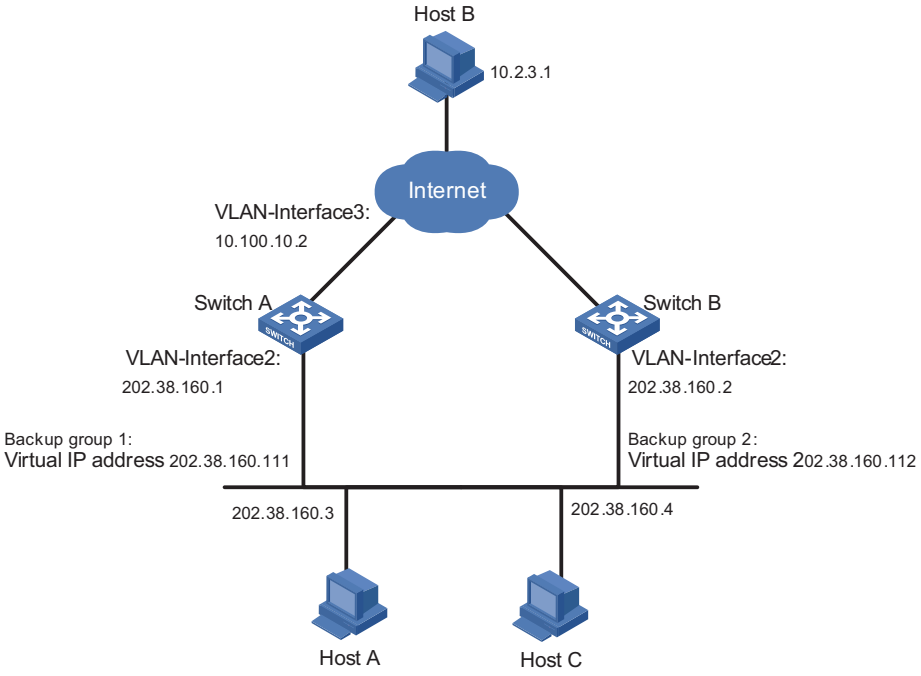
A switch can function as backup switches of multiple backup groups.

Multiple-backup group configuration can implement load balancing. For example, Switch A operates as the master switch of backup group 1 and a backup switch in backup group 2. Similarly, Switch B operates as the master switch of backup group

2 and a backup switch in backup group 1. Some hosts in the network take virtual router 1 as the gateway, while others take virtual router 2 as the gateway. In this way, both load balancing and mutual backup are implemented.

Network diagram

Figure 145 Network diagram for multiple-VRRP backup group configuration



Configuration procedure

- Configure Switch A.

Configure VLAN 2.

```
<LSW-A> system-view
[LSW-A] vlan 2
[LSW-A-vlan2] port Ethernet 1/0/6
[LSW-A-vlan2] quit
[LSW-A] interface Vlan-interface 2
[LSW-A-Vlan-interface2] ip address 202.38.160.1 255.255.255.0
```

Create backup group 1.

```
[LSW-A-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
```

Set the priority for backup group 1.

```
[LSW-A-Vlan-interface2] vrrp vrid 1 priority 150
```

Create backup group 2.

```
[LSW-A-Vlan-interface2] vrrp vrid 2 virtual-ip 202.38.160.112
```

- Configure Switch B.

Configure VLAN 2.

```
<LSW-B> system-view
[LSW-B] vlan 2
[LSW-B-vlan2] port Ethernet 1/0/6
[LSW-B-vlan2] quit
[LSW-B] interface Vlan-interface 2
[LSW-B-Vlan-interface2] ip address 202.38.160.2 255.255.255.0
```

Create backup group 1.

```
[LSW-B-Vlan-interface2] vrrp vrid 1 virtual-ip 202.38.160.111
```

Create backup group 2.

```
[LSW-B-Vlan-interface2] vrrp vrid 2 virtual-ip 202.38.160.112
```

Set the priority for backup group 2.

```
[LSW-B-Vlan-interface2] vrrp vrid 2 priority 110
```



Normally, multiple backup groups are used in actual use.

Troubleshooting VRRP

You can locate VRRP problems through the configuration and debugging information. Here are some possible failures you might meet and the corresponding troubleshooting methods.

Symptom 1: Frequent prompts of configuration errors on the console

This indicates that incorrect VRRP packets are received. It may be because of the inconsistent configuration of the switches within the backup group, or the attempt of other devices sending out illegal VRRP packets. The first possible fault can be solved through modifying the configuration. And as the second possibility is caused by the malicious attempt of some devices, non-technical measures should be resorted to.

Symptom 2: More than one master existing within a backup group

There are also 2 reasons. One is short time coexistence of many master switches, which is normal and needs no manual intervention. Another is the long time coexistence of many master switches, which may be because the original master switch and other member switches in a backup group cannot receive VRRP packets from each other, or receive some illegal packets.

To solve such a problem, an attempt should be made to ping among these masters and if such an attempt fails, check the connectivity between related devices. If they can be pinged through, check VRRP configuration. For the configuration of a VRRP backup group, complete consistency for the number of virtual IP addresses, each virtual IP address, timer duration and authentication type configured on each member switch must be guaranteed.

Symptom 3: VRRP state of a switch changes repeatedly

Such problems occur when the backup group timer duration is too short. They can be solved through prolonging the duration or configuring the preemption delay period.

53 HA CONFIGURATION

HA Overview

The Switch 7758 supports high availability (HA) feature. This feature is to achieve a high availability of the system and to recover the system as soon as possible in the event of failures so as to shorten the mean time between failures (MTBF) of the system.

The functions of HA are mainly implemented by the application running on Fabric module. A Switch 7758 has two Fabrics which are working in the master-slave mode: one module works in master mode as the master module, the other works in slave mode as a backup module. If the master-slave system detects a fault in the master module, a hot master-slave switchover will be performed automatically. The slave module will try to connect and control the system bus while the original master module will try to disconnect with the bus. Thus, the master-slave switchover of the active system is completed, and at the same time the original master module is reset to function as the slave module. Therefore, even if the master module fails, the slave module can also take its role to ensure that the Switch 7758 runs normally.

The Switch 7758 supports hot swap of Fabrics. The hot swap of master modules will cause switchover master/slave.

The Switch 7758 supports manually switchover master/slave. You can change the current module state manually by executing command.



CAUTION: *The HA feature of the Switch 7758 can detect the software upgrade of the two Fabric with at least one Fabric being active. However, the Fabric and the I/O Module of the Ethernet switches must be identical in their software version, otherwise they cannot work normally. So that during the upgrade, you are recommended to restart the whole switch after the Fabric executes the* ***boot boot-loader*** *command, to ensure the normal operating of the switch.*

The configuration file of the slave module is copied from the master module in real time, which can ensure that the slave system continues to operate in the same configuration as that of the original active system after the master-slave switchover. The Switch 7758 supports automatic synchronization of configuration file. The active system stores its configuration file and backup the configuration file to the slave system simultaneously when the master's configuration file is modified, so as to ensure the consistency of the configurations of the active system and slave system. And you can also use command to manually synchronize the configuration file of the master and slave module.

Besides, the system can monitor the power supply and the operating environment of the system and give timely alarms to avoid the escalation of failures and ensure safe operations of the system.

HA Configuration

HA Configuration Overview

Table 438 HA configuration tasks overview

Configuration	Description	Related section
Set the slave module restart manually	Required	"Setting the Slave Module Restart Manually" on page 568
Perform the master-slave switchover manually	Required	"Performing the Master-Slave Switchover Manually" on page 568
Enable automatic synchronization	Required	"Enabling Automatic Synchronization" on page 569
Synchronize the configuration file of the system manually.	Required	"Synchronizing the Configuration File of the System Manually" on page 569



- *When the Switch 7758 starts, if you log in to the slave module, it will take about 3 minutes before you can see the system prompt. During the 3 minutes, the slave module does not response to any operation. This is system protective design for avoiding switching shake.*
- *You cannot execute any command on the slave module until the slave module switches over to the master.*
- *The master module will batch backup the configuration to slave module as soon as the system is up, which is a quick action. During this action, the system will give prompt on both master module and slave module if you press the "enter" key on the terminal, at the time, you cannot execute any command on the master module. After the batch backup, the master module keeps doing the real-time backup to the slave and you can execute all commands on the master module.*
- *You must keep the consistency of the version of the master and slave module.*

Setting the Slave Module Restart Manually

When the slave module works normally, you can set the slave system restart manually.

Perform the following configuration in user view.

Table 439 Set slave module restart manually

Operation	Command	Description
Set slave module restart manually	**slave restart**	Optional

Performing the Master-Slave Switchover Manually

When the slave module is available and the master is in real-time backup state, you can inform the slave module of a master-slave switchover by using a command if you expect the slave module to operate in place of the master module. After the switchover, the slave module will control the system and the original master module will reset automatically.

Perform the following configuration in user view.

Table 440 Perform the master-slave switchover manually

Operation	Command	Description
Perform the master-slave switchover manually	**slave switchover**	Optional

Enabling Automatic Synchronization

The Switch 7758 supports automatic synchronization. The master module stores its configuration file and backups the configuration file to the slave module simultaneously when the master's configuration file is modified, so as to ensure the consistency of the configurations of the master system and slave system.

You can enable/disable automatic synchronize of the Switch 7758.

Perform the following configuration in system view.

Table 441 Enable automatic synchronization

Operation	Command	Description
Enter system view	**system-view**	-
Enable automatic synchronization	**slave auto-update config**	Optional

Synchronizing the Configuration File of the System Manually

The system can synchronize the configuration files on the master and slave modules automatically. If you want to synchronize them yourself, you can do it manually by using the command below.

Perform the following configuration in user view.

Table 442 Synchronize the configuration file manually

Operation	Command	Description
Synchronize the configuration file manually	**slave update configuration**	Optional

This operation can backup the configuration file to the slave module only if the slave system operates normally. The configuration file will be fully copied at each time the operation is executed.

Displaying HA

After the above configuration, you can execute the **display** command in any view to view the HA configuration, and to verify the effect of the configuration.

Table 443 Display HA

Operation	Command	Description
Display the switchover status of the master/slave board	**display switchover state** [*slot-id*]	The **display** command can be executed in any view.

54 ARP CONFIGURATION

Introduction to ARP

Address Resolution Protocol (ARP) is used to map network layer protocol addresses (IP addresses) to corresponding data link layer hardware addresses (MAC addresses).

Necessity of ARP

Network devices can directly identify Layer 2 MAC addresses instead of Layer 3 IP addresses. For a Layer 3 packet to be received by its destination host, it must carry the MAC address of the destination host. So, before sending a packet, the source device must map the destination IP address to the MAC address of the destination device.

ARP Packet Format

There are two types of ARP packets: ARP request and ARP reply. Figure 146 illustrates the structure of the two types of ARP packets. In this figure:

- All fields except for the target hardware address field are used in an ARP request. The target hardware address is just what the sender wants to obtain.
- All fields are used in an ARP reply.

Figure 146 ARP packet format

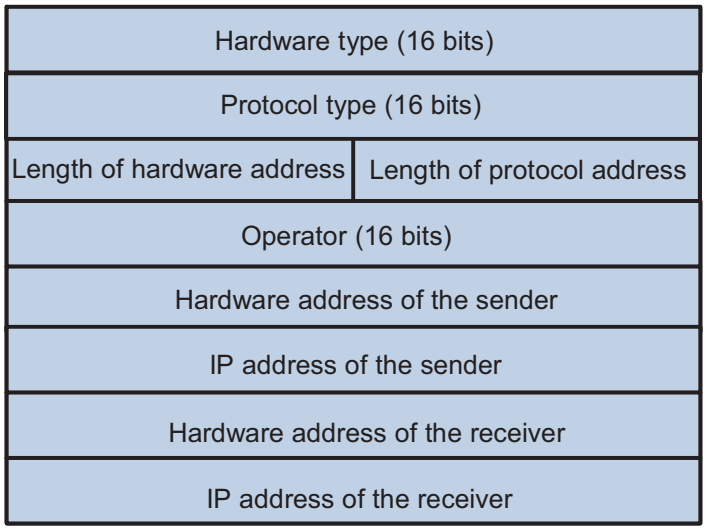


Table 444 describes the fields of an ARP packet.

Table 444 Field descriptions of an ARP packet

Field	Description
Hardware Type	Type of the hardware interface. See Table 445 for the valid values of this field.

Table 444 Field descriptions of an ARP packet

Field	Description
Protocol type	Type of the protocol address to be mapped. For IP address, the value of this field is 0x0800.
Hardware address length	Length of the hardware address (in bytes)
Protocol address length	Length of the protocol address (in bytes)
Operation code	Type of the packet, which can be: ■ 1: ARP request ■ 2: ARP reply ■ 3: RARP request ■ 4: RARP reply
Sender hardware address	Hardware address of the sender
Sender IP address	IP address of the sender
Target hardware address	This field is null for an ARP request, and is the hardware address of the receiver for an ARP reply.
Target IP address	IP address of the receiver

Table 445 Values of the hardware type field

Value	Description
1	Ethernet
2	Experimental Ethernet
3	X.25
4	Proteon ProNET (Token Ring)
5	Chaos
6	IEEE 802.x
7	ARC network

ARP Table

In an Ethernet network, two hosts must know each other's MAC address for them to communicate with each other. For this reason, each host on the network maintains an ARP table, which contains some lately used IP address-to-MAC address mapping entries. Note that this manual only introduces basic implementation of ARP table. Different manufactures' products may provide more information about ARP table. On a Switch 7750 Ethernet switch, you can use the **display arp** command to display ARP table entries.

Table 446 describes the fields of APR table.

Table 446 Field descriptions of an ARP table

Field	Description
IF index	Index of the physical interface or port on the device owning the physical address and IP address in the entry
Physical address	Physical address of the device, a MAC address
IP address	IP address of the device

Table 446 Field descriptions of an ARP table

Field	Description
Type	Entry type, which can be: ■ 1: Not any of the following ■ 2: Invalid entry ■ 3: Dynamic entry ■ 4: Static entry

ARP Implementation

The ARP table of a host is empty when the host just starts up. When a dynamic ARP entry has not been used for a specific time period, it is removed from the ARP table. The purpose of this is to save memory space and update the entries in the ARP table. The following describes the implementation procedure of ARP.

- Suppose Host A and Host B are on the same network segment. The IP address of Host A is IP_A and that of Host B is IP_B. To send a packet to Host B, Host A first looks up its own ARP table for an ARP entry that contains IP_B. If such an entry is found, Host A encapsulates the IP packet into a frame by using the MAC address in the entry as the destination MAC address and then sends the frame to Host B.
- If no such an entry is found in the ARP table, Host A puts the packet into the transmission queue, generates an ARP request packet with the IP addresses of Host B and Host A and the MAC address of Host A (IP_B, IP_A and MAC_A), and broadcasts the request on the Ethernet. Since the ARP request is broadcasted, all hosts on the network segment receive it. However, only the host with IP address IP_B (Host B) will process the request further.
- Host B adds the sender IP address and MAC address carried in the request (IP_A and MAC_A of Host A) in an entry to its ARP table and then returns an ARP reply packet to the sender (Host A), with its MAC address carried in the packet. Note that the ARP reply is a unicast packet instead of a broadcasted packet.
- Upon receiving the ARP reply, Host A extracts the IP address and MAC address of Host B from the packet, adds them in an entry to its ARP table, and then sends out all the packets destined for Host B in the transmission queue.

Generally, a host will automatically trigger ARP procedure during IP addressing.

Introduction to Gratuitous ARP

Gratuitous ARP packets have the following characteristics:

- Both source and destination IP addresses of a gratuitous ARP packet are the local addresses; the source MAC address of it is the local MAC address.
- If a device finds that the IP address in an incoming gratuitous packet conflicts with its own IP address, it returns an ARP replay to the sending device to notify the sender of the IP address conflict.

By sending gratuitous ARP packets, a network device can:

- Determine whether or not IP address conflict exists between it and other network devices.
- Trigger other network devices to update its hardware address stored in their caches.

With gratuitous ARP learning enabled on a device, each time the device receives a gratuitous ARP packet, the device updates the ARP entry matching the packet in the cache (if exists) by using the hardware address of the sender carried in the gratuitous ARP packet.

Overview of gratuitous ARP update interval

When ARP aging timer expires, some hosts in the network directly delete the ARP entries learned dynamically, incapable of updating ARP entries actively. These hosts have to trigger a new ARP request packet with a new IP packet received to request for the gateway address. As a host can buffer only one packet, when a ping is sent with a long packet, multiple fragments will be lost, which interrupts the ping.

When network load or the CPU occupancy of the receiving host is high, ARP packets may be lost or the host may be unable to process the ARP received timely. In such a case, after the dynamic ARP entries on the host age out, the traffic between the host and the sending device will remain interrupted before the host learns the ARP entries on the sending device again.

To address this issue, you can configure the gratuitous ARP update interval on the Switch 7750 Ethernet switches. With gratuitous ARP packets sent periodically, the receiving host can update the ARP entry for the gateway in its ARP table timely. In this way, the ARP entry for the gateway has been updated before the host ages out the entry; therefore, this entry will not be deleted. This prevents traffic interruption as mentioned above.

How gratuitous ARP update interval works

A switch periodically sends gratuitous ARP packets that carry the master IP address and secondary IP address of VLAN interfaces and the IP addresses of all the VRRP virtual routers to update the ARP entries on the device that is connected to the switch and incapable of updating ARP entries actively.

If a small number of VLAN interfaces and VRRP backup groups are configured, it takes a very time for the device to traverse all the VLAN interfaces and their IP addresses. If the traffic loops without being limited, gratuitous ARP packets are sent to the same IP address at an interval too short. This increases switch work load and network traffic. To solve this problem, the device allows you to configure the gratuitous ARP update interval.

Introduction to ARP Attack Detection

If an attacker sends an ARP message with a fake source IP address to a gateway, the gateway adds the IP-to-MAC mapping into its ARP mapping table. The attacker may send ARP messages with all the IP addresses of the network segment as the source IP addresses to the gateway, causing other devices unable to access the network.

To guard against such attacks, Switch 7750 Ethernet switches support the ARP attack detection feature. With this feature, you can limit the number of IP addresses to be bound to a MAC address in a VLAN. If a MAC address is bound to more than the specified number of IP addresses, it is considered an attacking MAC address. Consequently, all the ARP messages containing the attacking MAC address as the source MAC address will be discarded unless the ARP request is sent from the local device.

Introduction to ARP Packet Rate Limit

If an attacker sends a large number of ARP packets to a port of a switch, the CPU will get overloaded, causing other functions to fail, and even the whole device to break down. To guard against such attacks, Switch 7750 Ethernet switches support the ARP packets rate limit function, which can disable the attacked port from receiving any packet temporarily, thus preventing serious impact on the CPU.

With this function enabled on a port, the switch will count the ARP packets received on the port within each second. If the number of ARP packets received on the port per second exceeds the preconfigured value, the switch considers that the port is being attacked by ARP packets. In this case, the switch disables the port from receiving any packet, generates an alarm message, and logs the event. At the same time, the switch continues to count the ARP packets on the port. If the number of received ARP packets remains under the preconfigured value for a certain period (port state auto-recovery interval), the port will revert to the Up state.

Switch 7750 Ethernet switches support configuring trusted ports for ARP packet rate limit. A switch does not count ARP packets or limit ARP packets received on a trusted port.

Introduction to ARP Source Suppression

With the ARP source suppression function, the switch classifies incoming ARP packets and limits the maximum number of ARP packets with the same type that can be sent to the CPU in a time of time, so as to protect the CPU from being attacked by illegal ARP packets generated by ARP scanning of a host to the whole network.

A Switch 7750 classifies incoming ARP packets into the following types:

- Arbitrary ARP packets, whose source/destination IP addresses are not distinguished
- Pass-through ARP packets, whose source IP addresses are the same one and destination IP addresses are not the IP address of the current switch
- Locally-terminated ARP packets, whose source IP addresses are the same one and destination addresses are the IP address of the current switch.

For each type, you can set the maximum number of ARP packets that can be sent to the CPU in a unit of time on the switch. When the number of ARP packets received in a unit of time exceeds the corresponding setting, the switch will regard the exceeding ones as illegal ARP packets and discard them.

Configuring ARP

ARP entries in a Switch 7750 can be one of two types; static or dynamic, as described in Table 447.

Table 447 ARP entry

ARP entry	Generation method	Maintenance method
Static ARP entry	Manually configured	Manual maintenance
Dynamic ARP entry	Dynamically generated	A dynamic ARP entry ages out when ARP aging timer expires.

Configuration Tasks

Table 448 ARP configuration tasks

Configuration task	Description	Related section
Add a static ARP entry manually	Optional	"Adding a Static ARP Entry Manually" on page 576
Configure the maximum number of ARP entries that can be learnt	Optional	"Configuring the Maximum Number of ARP Entries that Can Be Learnt" on page 576
Configure the aging timer for dynamic ARP entries	Optional	"Configuring the Aging Time for Dynamic ARP Entries" on page 577
Configure ARP entry checking	Optional	"Configuring ARP Entry Checking" on page 577
Enabling ARP forwarding in the protocol-based VLAN	Optional	"Enabling ARP Forwarding in the Protocol-Based VLAN" on page 577
Configure gratuitous ARP	Optional	"Configuring Gratuitous ARP" on page 578
Configure ARP attack detection	Optional	"Configuring ARP Attack Detection" on page 578
Configure ARP packet rate limit	Optional	"Configuring ARP Packet Rate Limit" on page 578
Configure ARP source suppression	Optional	"Configuring ARP Source Suppression" on page 579

Adding a Static ARP Entry Manually

Table 449 Add a static ARP entry manually

Operation	Command	Description
Enter system view	**system-view**	-
Add a static ARP entry manually	**arp static** *ip-address mac-address* [*vlan-id interface-type interface-number*]	Required By default, there is no static ARP entry in the ARP table, and ARP entries are dynamically created by ARP.



CAUTION:

- *Static ARP entries are valid as long as the Ethernet switch operates normally, unless they are removed as the results of some operations, like changing/removing a VLAN interface, removing a VLAN, and removing a port from a VLAN.*
- *The VLAN specified by the vlan-id argument in the **arp static** command must be an existing VLAN, and the port specified by the interface-type and interface-number arguments must belong to the VLAN.*

Configuring the Maximum Number of ARP Entries that Can Be Learnt

Table 450 Configure the maximum number of ARP entries that can be learnt on a port

Operation	Command	Description
Enter system view	**system-view**	-
Configure the total maximum number of ARP entries	**arp max-entry** *number*	Optional It is 8192 by default.

Table 450 Configure the maximum number of ARP entries that can be learnt on a port

Operation	Command	Description
Enter port view	**interface** *interface-type interface-number*	-
Configure the maximum number of dynamic ARP entries that can be learnt by the port	**arp max-dynamic-entry** *number*	Optional It is 2048 by default.

Configuring the Aging Time for Dynamic ARP Entries

Table 451 Configure the aging time for dynamic ARP entries

Operation	Command	Description
Enter system view	**system-view**	-
Configure the aging time for dynamic ARP entries	**arp timer aging** *aging-time*	Optional By default, this time is 20 minutes.

Configuring ARP Entry Checking

Table 452 Enable ARP entry checking

Operation	Command	Description
Enter system view	**system-view**	-
Enable ARP entry checking to disable the switch from learning ARP entries with multicast MAC addresses	**arp check enable**	Optional By default, the function is enabled and no multicast MAC address ARP entry will be learnt.

Enabling ARP Forwarding in the Protocol-Based VLAN

The system allows for classifying VLANs based on protocols, and such VLANs are called protocol-based VLANs. For details, refer to *"Protocol-Based VLAN" on page 91*. After you enable ARP in a protocol-based VLAN, the switch can forward ARP packets through the receiving interfaces based on the operating mechanism. However, this may affect other devices to learn ARP entries in practice.

To prevent the switch from forwarding ARP requests out the receiving interfaces, you need to disable ARP and disable ARP forwarding in the protocol-based VLAN.

For commands about disabling ARP in a protocol-based VLAN, refer to "Protocol-Based VLAN" on page 91.

Table 453 Enable ARP forwarding in the protocol-based VLANs

Operation	Command	Description
Enter system view	**system-view**	-
Enable ARP forwarding in the protocol-based VLAN(s)	**arp relay enable**	Optional By default, the feature is enabled.



CAUTION: *Since the close relation between IP and ARP, disabling ARP or ARP forwarding in a protocol-based VLAN may cause incorrect IP-to-MAC resolutions.*

Configuring Gratuitous ARP

Configuring Gratuitous ARP Learning

Table 454 Enable gratuitous ARP learning

Operation	Command	Description
Enter system view	**system-view**	-
Enable gratuitous ARP learning	**gratuitous-arp-learning enable**	Required Disabled by default.

Configuring the Gratuitous ARP Update Interval

Table 455 Configure the gratuitous ARP update interval

Operation	Command	Description
Enter system view	**system-view**	-
Enable gratuitous ARP packets to be sent periodically	**arp gratuitous-updating enable**	Required By default, this function is disabled on the switch.
Set a gratuitous ARP update interval	**arp timer gratuitous-updating** *updating-interval*	Optional The gratuitous ARP update interval defaults to five minutes after this function is enabled.

With VRRP enabled on a VLAN interface of a switch

- *If the switch is the master switch, it sends gratuitous ARP messages with the IP address of the VRRP virtual router.*
- *If it is not the master switch, it sends gratuitous ARP messages with the primary and all the secondary IP addresses of the VLAN interface.*

Configuring ARP Attack Detection

Table 456 Configure ARP attack detection

Operation	Command	Description
Enter system view	**system-view**	-
Set the maximum number of IP addresses to be bound to a MAC address in a VLAN	**arp mac-arp-map limit** *number*	Required By default, the maximum number is 2.

If secondary IP addresses are configured for a VLAN interface, the specified maximum number of IP addresses to be bound to a MAC address should be bigger than the total number of the primary and secondary IP addresses of the VLAN interface.

Configuring ARP Packet Rate Limit

Table 457 Configure the ARP packet rate limit function

Operation	Command	Description
Enter system view	**system-view**	-
Enable the ARP packet rate limit function	**arp rate-limit enable**	Required Disabled by default.

Table 457 Configure the ARP packet rate limit function

Operation	Command	Description
Configure the maximum ARP packet receive rate on the port	**arp rate-limit** *rate*	Optional By default, the maximum ARP packet receive rate on a port is 15pps.
Configure the port state auto-recovery interval	**arp protective-down recover interval** *time*	Optional 300 seconds by default.
Configure the port as a trusted port for ARP packet rate limit	**arp rate-limit trust**	Optional By default, the port is an untrusted port.

Configuring ARP Source Suppression

By setting the maximum numbers of ARP packets of different types that can be sent to the CPU in a unit of time, you can protect the CPU from being attacked by illegal ARP packets.

Table 458 Configure ARP source suppression

Operation	Command	Description
Enter system view	**system-view**	-
Configure the maximum number of ARP packets of a type that can be sent to the CPU in a unit of time	**arp source-suppression limit** { **total** | **local** | **through** } *limit-value*	Optional The default value varies with the type of ARP packets ■ When **total** is adopted, the default value is 100. ■ When **local** is adopted, the default value is 3. ■ When **through** is adopted, the default value is 3.

Displaying and Maintaining ARP Configuration

After the above configuration, execute the **display** command in any view to display and verify the ARP configuration.

Execute the **reset** command in user view to clear ARP entries.

Table 459 Display and maintain ARP configuration

Operation	Command	Description
Display ARP attack information	**display arp attack-list**	You can execute the **display** command in any view.
Display ARP entries	**display arp** [**static** | **dynamic** | *ip-address*]	
Display the ARP entries matching a specified rule	**display arp** | { **begin** | **include** | **exclude** } *text*	
Display the number limits of ARP entries	**display arp entry-limit** [*interface-type interface-number*]	
Display the ARP entries of all ports on a specified slot	**display arp slot** *slot-id*	
Display the ARP entries of all ports in a specified VLAN	**display arp vlan** *vlan-id*	
Display the ARP entries of a specified interface	**display arp interface** *interface-type interface-number*	
Display ARP packet rate limit configuration information	**display arp rate-limit**	
Display the setting for ARP aging timer	**display arp timer aging**	
Display information about ARP source suppression	**display arp source-suppression**	
Clear ARP entries	**reset arp** [**dynamic** | **static** | **interface** *interface-type interface-number*]	You can execute the **reset** command in user view.
Clear the ARP attack information	**reset arp attack-list**	

ARP Configuration Example

Basic ARP Configuration Example

Network requirements

- Disable the ARP entry checking function.
- Enable the switch to send gratuitous ARP packets periodically.
- Set the aging time for dynamic ARP entries to 10 minutes.
- Add a static ARP entry with IP address 192.168.1.1, MAC address 000f-e201-0000, and outbound port Ethernet 2/0/10 of VLAN 1.

Configuration procedure

```
<SW7750> system-view
[SW7750] undo arp check enable
[SW7750] arp gratuitous-updating enable
[SW7750] arp timer aging 10
[SW7750] arp static 192.168.1.1 000f-e201-0000 1 Ethernet2/0/10
```

ARP Packet Rate Limit Configuration Example

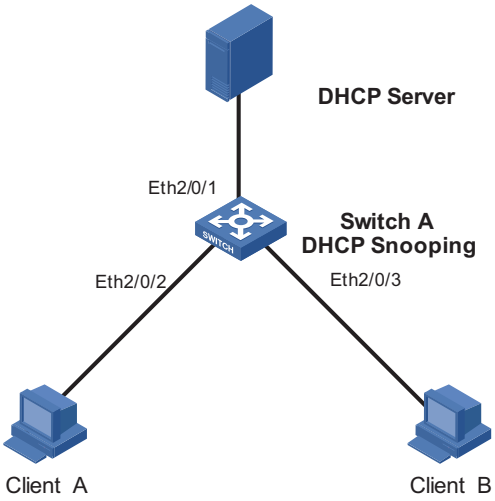
Network requirements

As shown in Figure 147, Ethernet 2/0/1 of Switch A connects to DHCP Server; Ethernet 2/0/2 connects to Client A, Ethernet 2/0/3 connects to Client B. Ethernet 2/0/1, Ethernet 2/0/2 and Ethernet 2/0/3 belong to VLAN 1.

- Enable DHCP snooping on Switch A and specify Ethernet 2/0/1 as the trusted port for DHCP snooping and ARP packet rate limit.
- Enable the ARP packet rate limit function, so as to prevent Client A and Client B from attacking Switch A through ARP traffic.
- Enable the port state auto recovery function on the ports of Switch A, and set the recovery interval to 200 seconds.

Network diagram

Figure 147 ARP packet rate limit configuration



Configuration procedure

Enable DHCP snooping on Switch A.

```
<SwitchA> system-view
[SwitchA] dhcp-snooping
```

Specify Ethernet 2/0/1 as the trusted port for DHCP snooping and ARP packet rate limit.

```
[SwitchA] interface Ethernet2/0/1
[SwitchA-Ethernet2/0/1] dhcp-snooping trust
[SwitchA-Ethernet2/0/1] arp detection trust
[SwitchA-Ethernet2/0/1] quit
```

Enable the ARP packet rate limit function, and set the maximum ARP packet rate allowed on the port to 20 pps.

```
[SwitchA] arp rate-limit enable
[SwitchA] arp rate-limit 20
```

Configure the port state auto recovery function, and set the recovery interval to 200 seconds.

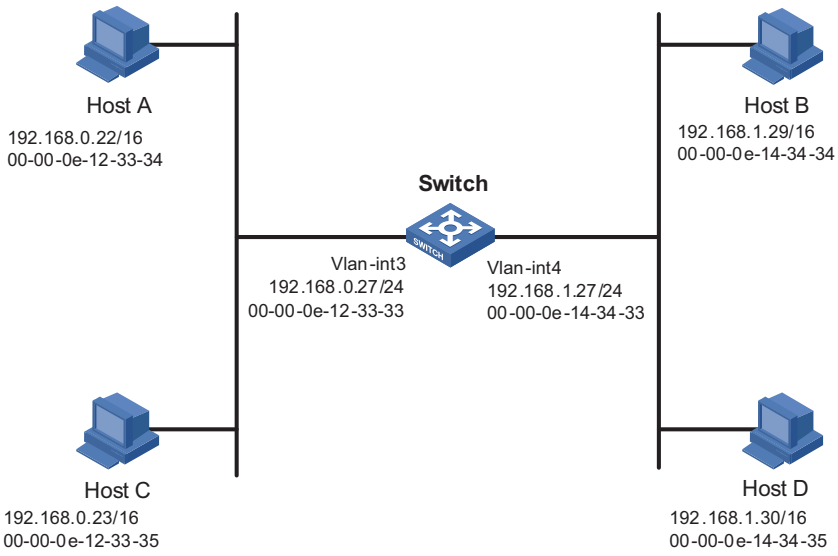
```
[SwitchA] arp protective-down recover interval 200
```

55 PROXY ARP CONFIGURATION

Proxy ARP Overview

Proxy ARP allows hosts that have IP addresses of the same network segment but reside on different physical networks to communicate with each other through ARP.

Figure 148 Work mechanism of proxy ARP



As shown in Figure 148:

From the perspective of the switch, Host A and Host D reside on different networks. However, when Host A (192.168.0.22/16) needs to send packets to Host D (192.168.1.30/16), it finds they are on the same network 192.168.0.0/16, and thus Host A will broadcast an ARP request to request the MAC address of Host D.

- When the proxy ARP feature is not enabled on the switch, because Host A and Host D are in different VLANs, the ARP request sent by Host A cannot reach Host D, and the two hosts cannot communicate.
- With proxy ARP enabled on the switch, when VLAN-interface 3 receives the ARP request, if the switch finds a route to the destination IP address (encapsulated in the ARP request) in the routing table, the switch sends host A the MAC address (00-00-0e-12-33-33) of VLAN-interface 3 in an ARP response (with the source IP address being the destination IP address of the ARP request). After receiving the ARP response, Host A creates an ARP entry, in which the destination IP address is the IP address of Host D (192.168.1.30/16), and the MAC address is that of VLAN-interface 3 (00-00-0e-12-33-33). The subsequent packets sent from Host A to Host D will all be sent to

VLAN-interface 3 of the switch, and then the switch routes the packets to Host D, so as to realize the Layer 3 connectivity between Host A and Host D.

Proxy ARP is needed in the following cases (hosts have IP addresses of the same network segment).

- For hosts in different VLANs on a Switch 7750 to communicate, you need to enable proxy ARP on the VLAN interfaces.
- For hosts in different sub-VLANs of a super VLAN on a Switch 7750 to communicate, you need to enable proxy ARP on the super VLAN interface.
- For hosts in different secondary VLANs of an isolate-user-vlan on a Layer 2 switch that is connected to a Switch 7750 to communicate, you need to enable proxy ARP on the Switch 7750.



- *Generally, ports in the same VLAN are interconnected at Layer 2 by default. So, ARP proxy only processes inter-VLAN ARP requests and does not deal with intra-VLAN ARP requests.*
- *When isolate-user-vlan function is enabled on the Layer 2 switches connected with the Switch 7750, ports in the same VLAN are isolated with each other at Layer 2. To provide Layer 3 connectivity between Layer 2 isolated ports in the same VLAN, you need to enable the intra-VLAN ARP proxy function on the Switch 7750 to have ARP proxy process intra-VLAN ARP requests.*

Configuring Proxy ARP

Table 460 Configure proxy ARP

Operation	Command	Description
Enter system view	**system-view**	-
Enter VLAN interface view	**interface Vlan-interface** *vlan-id*	-
Enable proxy ARP	**arp proxy enable**	Required By default, proxy ARP is disabled.
Enable intra-VLAN proxy ARP	**arp proxy source-vlan enable**	Optional By default, intra-VLAN proxy ARP is disabled, and the proxy ARP only processes inter-VLAN ARP requests.
Display the status of ARP proxy	**display arp proxy** [**interface** *interface-type interface-number*]	Available in any view

Proxy ARP Configuration Example

Proxy ARP Configuration Example

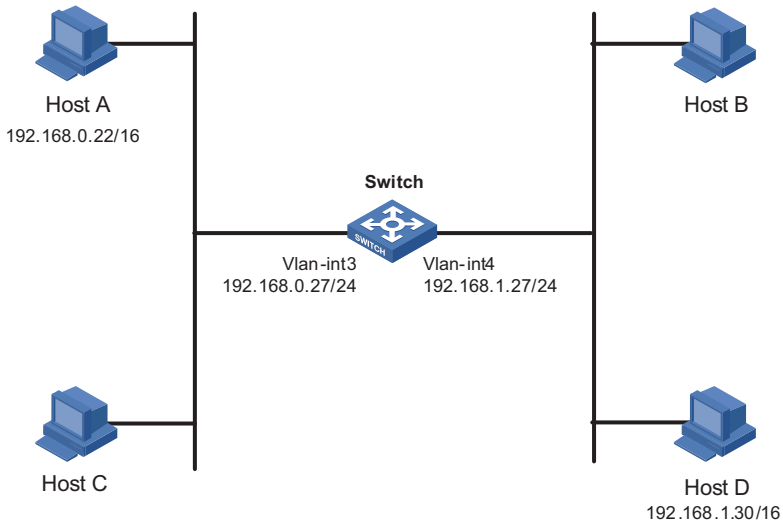
Network requirements

- The IP address of PC A is 192.168.0.22/16, and that of PC D is 192.168.1.30/16.
- Create VLAN 3 and VLAN 4 on the switch.

- Configure the IP address of VLAN-interface 3 as 192.168.0.27/24, and that of VLAN-interface 4 as 192.168.1.27/24.
- Enable proxy ARP on VLAN-interface 3 and VLAN-interface 4 to allow Host A and Host D to communicate with each other through ARP.

Network diagram

Figure 149 Network diagram for proxy ARP



Configuration procedure

Configure the IP address of VLAN-interface 3 as 192.168.0.27/24.

```
<Switch> system-view
[Switch] interface Vlan-interface 3
[Switch-Vlan-interface3] ip address 192.168.0.27 24
[Switch-Vlan-interface3] quit
```

Configure the IP address of VLAN-interface 4 as 192.168.1.27/24

```
[Switch] interface Vlan-interface 4
[Switch-Vlan-interface4] ip address 192.168.1.27 24
[Switch-Vlan-interface4] quit
```

Enable proxy ARP on VLAN-interface 3.

```
[Switch] interface Vlan-interface 3
[Switch-Vlan-interface3] arp proxy enable
[Switch-Vlan-interface3] quit
```

Enable proxy ARP on VLAN-interface 4.

```
[Switch] interface Vlan-interface 4
[Switch-Vlan-interface4] arp proxy enable
[Switch-Vlan-interface4] quit
```

Super VLAN Proxy ARP Configuration Example

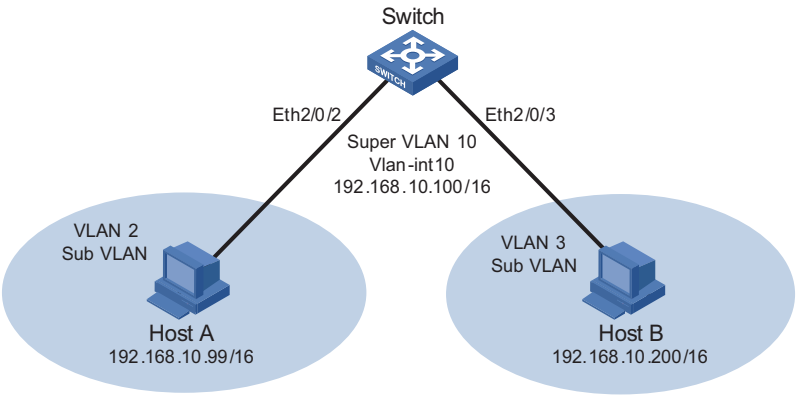
Network requirements

- Create a super VLAN, VLAN 10 and configure the IP address of VLAN-interface 10 as 192.168.10.100/16.

- Create Sub-VLANs (VLAN 2 and VLAN 3).
- Ethernet 2/0/2 belongs to VLAN 2 and Ethernet 2/0/3 belongs to VLAN 3.
- Enable proxy ARP on VLAN-interface 10 to allow Host A (in VLAN 2) and Host B (in VLAN 3) to communicate with each other through ARP.

Network diagram

Figure 150 Network diagram for ARP in super VLAN



Configuration procedure

Create the super VLAN and the sub-VLANs. Add Ethernet 2/0/2 to VLAN 2 and Ethernet 2/0/3 to VLAN 3. Configure the IP address 192.168.10.100/16 for VLAN-interface 10.

```
<Switch> system-view
[Switch] vlan 2
[Switch-vlan2] port ethernet 2/0/2
[Switch-vlan2] quit
[Switch] vlan 3
[Switch-vlan3] port ethernet 2/0/3
[Switch-vlan3] quit
[Switch] vlan 10
[Switch-vlan10] supervlan
[Switch-vlan10] subvlan 2 3
[Switch-vlan10] interface vlan-interface 10
[Switch-Vlan-interface10] ip address 192.168.10.100 255.255.0.0
[Switch-Vlan-interface10] quit
```

Enable proxy ARP on VLAN-interface 10 to allow Host A and Host B to communicate with each other through ARP.

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] arp proxy enable
[Switch-Vlan-interface10] quit
```

Isolate-user-vlan Proxy ARP Configuration Example

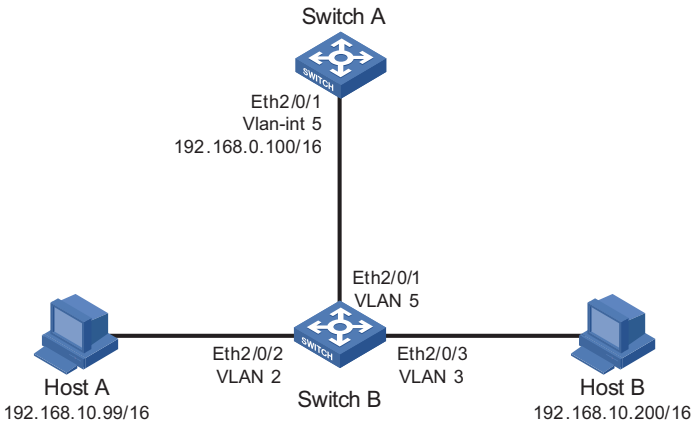
Network requirements

- Switch A is connected to Switch B through Ethernet 2/0/1.
- VLAN 5 on Switch B is an isolate-user-vlan, which contains uplink port Ethernet 2/0/1 and two secondary VLANs (VLAN 2 and VLAN 3). Ethernet 2/0/2 belongs to VLAN 2, and Ethernet 2/0/3 belongs to VLAN 3.

- Enable proxy ARP on Switch A to allow Host A (in VLAN 2) and Host B (in VLAN 3) to communicate with each other through ARP.

Network diagram

Figure 151 Network diagram for proxy ARP configuration in isolate-user-vlan



Configuration procedure

1 Configure Switch B

Create VLAN 2, VLAN 3, and VLAN 5 on Switch B. Add Ethernet 2/0/2 to VLAN 2, Ethernet 2/0/3 to VLAN 3, and Ethernet 2/0/1 to VLAN 5. Configure VLAN 5 as the isolate-user-vlan, and VLAN 2 and VLAN 3 as secondary VLANs. Configure the secondary VLANs to belong the isolate-user-vlan.

```
<SwitchB> system-view
[SwitchB] vlan 2
[SwitchB-vlan2] port ethernet 2/0/2
[SwitchB-vlan2] quit
[SwitchB] vlan 3
[SwitchB-vlan3] port ethernet 2/0/3
[SwitchB-vlan3] quit
[SwitchB] vlan 5
[SwitchB-vlan5] port ethernet 2/0/1
[SwitchB-vlan5] isolate-user-vlan enable
[SwitchB-vlan5] quit
[SwitchB] isolate-user-vlan 5 secondary 2 3
```

2 Configure Switch A

Configure VLAN 5, and add Ethernet 2/0/1 to it.

```
<SwitchA> system-view
[SwitchA] vlan 5
[SwitchA-vlan5] port ethernet 2/0/1
[SwitchA-vlan5] interface vlan-interface 5
[SwitchA-Vlan-interface5] ip address 192.168.10.100 255.255.0.0
```

Enable proxy ARP and intra-VLAN ARP on VLAN-interface 5 to allow Host A and Host B to communicate with each other through ARP.

```
[SwitchA-Vlan-interface5] arp proxy enable
[SwitchA-Vlan-interface5] arp proxy source-vlan enable
[SwitchA-Vlan-interface5] quit
```

56 DHCP Overview

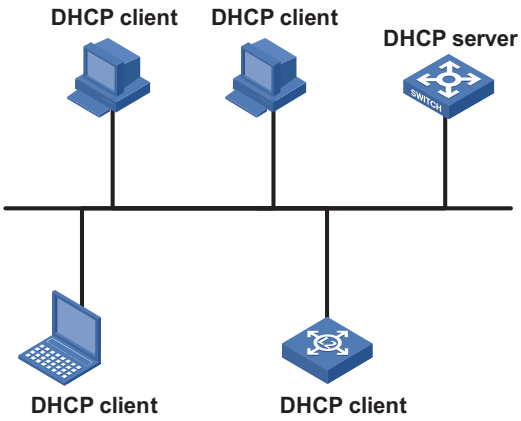
Introduction to DHCP

With networks getting larger in size and more complicated in structure, lack of available IP addresses becomes the common situation the network administrators have to face, and network configuration becomes a tough task for the network administrators. With the emerging of wireless networks and the using of laptops, the position change of hosts and frequent change of IP addresses also require new technology. Dynamic host configuration protocol (DHCP) is developed in this background.

DHCP adopts a client/server model, where DHCP clients send requests to DHCP servers for configuration parameters; and the DHCP servers return the corresponding configuration information such as IP addresses to configure IP addresses dynamically.

A typical DHCP application includes one DHCP server and multiple clients (such as PCs and laptops), as shown in Figure 152.

Figure 152 Typical DHCP application



DHCP IP Address Assignment

IP Address Assignment Policy

Currently, DHCP provides the following three IP address assignment policies to meet the requirements of different clients:

- Manual assignment. The administrator statically binds IP addresses to few clients with special uses (such as WWW server). Then the DHCP server assigns these fixed IP addresses to the clients.
- Automatic assignment. The DHCP server assigns IP addresses to DHCP clients. The IP addresses will be occupied by the DHCP clients permanently.

- Dynamic assignment. The DHCP server assigns IP addresses to DHCP clients for predetermined period of time. In this case, a DHCP client must apply for an IP address at the expiration of the period. This policy applies to most clients.

Obtaining IP Addresses Dynamically

A DHCP client undergoes the following four phases to dynamically obtain an IP address from a DHCP server:

1. Discover: In this phase, the DHCP client tries to find a DHCP server by broadcasting a DHCP-DISCOVER packet.
2. Offer: In this phase, the DHCP server offers an IP address. Each DHCP server that receives the DHCP-DISCOVER packet chooses an unassigned IP address from the address pool based on the IP address assignment policy and then sends a DHCP-OFFER packet (which carries the IP address and other configuration information) to the DHCP client. The transmission mode depends on the flag field in the DHCP-DISCOVER packet. For details, see "DHCP Packet Format" on page 590.
3. Select: In this phase, the DHCP client selects an IP address. If more than one DHCP server sends DHCP-OFFER packets to the DHCP client, the DHCP client only accepts the DHCP-OFFER packet that first arrives, and then broadcasts a DHCP-REQUEST packet containing the assigned IP address carried in the DHCP-OFFER packet.
4. Acknowledge: Upon receiving the DHCP-REQUEST packet, the DHCP server returns a DHCP-ACK packet to the DHCP client to confirm the assignment of the IP address to the client, or returns a DHCP-NAK packet to refuse the assignment of the IP address to the client. When the client receives the DHCP-ACK packet, it broadcasts an ARP packet with the assigned IP address as the destination address to detect the assigned IP address, and uses the IP address only if it does not receive any response within a specified period.



The IP addresses offered by other DHCP servers (if any) are not used by the DHCP client and are still available to other clients.

Updating IP Address Lease

After a DHCP server dynamically assigns an IP address to a DHCP client, the IP address keeps valid only within a specified lease time and will be reclaimed by the DHCP server when the lease expires. If the DHCP client wants to use the IP address for a longer time, it must update the IP lease.

By default, a DHCP client updates its IP address lease automatically by unicasting a DHCP-REQUEST packet to the DHCP server when half of the lease time elapses. The DHCP server responds with a DHCP-ACK packet to notify the DHCP client of a new IP lease if the server can assign the same IP address to the client. Otherwise, the DHCP server responds with a DHCP-NAK packet to notify the DHCP client that the IP address will be reclaimed when the lease time expires.

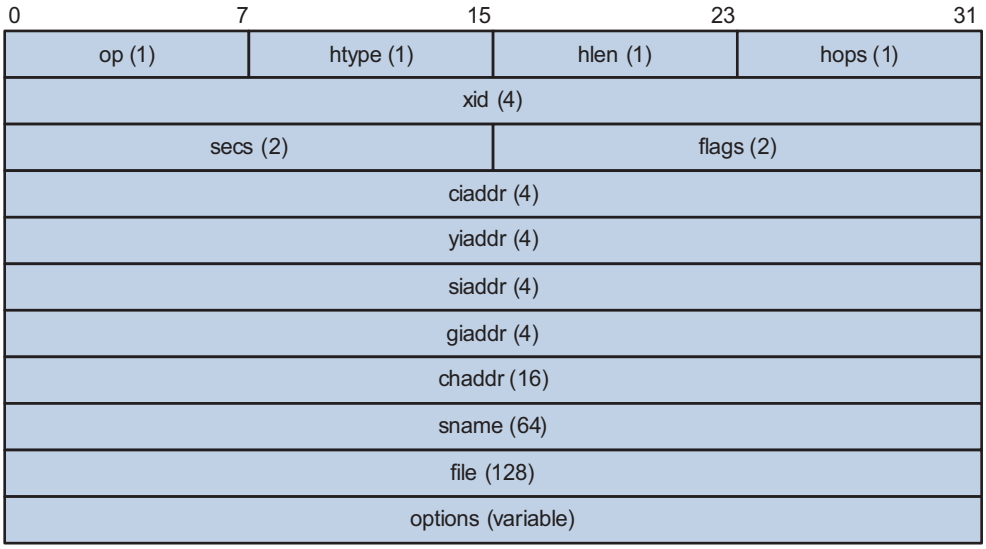
If the DHCP client fails to update its IP address lease when half of the lease time elapses, it will update its IP address lease by broadcasting a DHCP-REQUEST packet to the DHCP server again when seven-eighths of the lease time elapses. The DHCP server performs the same operations as those described in the previous section.

DHCP Packet Format

DHCP has eight types of packets. They have the same format, but the values of some fields in the packets are different. The DHCP packet format is based on that

of the BOOTP packets. The following table describes the packet format (the number in the brackets indicates the field length, in bytes):

Figure 153 Format of DHCP packets



The field meanings are illustrated as follows:

- op: Operation types of DHCP packets: 1 for request packets and 2 for response packets.
- htype, hlen: Hardware address type and length of the DHCP client.
- hops: Number of DHCP relay agents which a DHCP packet passes. For each DHCP relay agent that the DHCP request packet passes, the field value increases by 1.
- xid: Random number that the client selects when it initiates a request. The number is used to identify an address-requesting process.
- secs: Elapsed time after the DHCP client initiates a DHCP request.
- flags: The first bit is the broadcast response flag bit. It is used to identify that the DHCP response packet is sent in the unicast or broadcast mode. Other bits are reserved.
- ciaddr: IP address of a DHCP client.
- yiaddr: IP address that the DHCP server assigns to a client.
- siaddr: IP address of the DHCP server.
- giaddr: IP address of the first DHCP relay agent that the DHCP client passes after it sent the request packet.
- chaddr: Hardware address of the DHCP client.
- sname: Name of the DHCP server.
- file: Name of the start configuration file that the DHCP server specifies for the DHCP client.
- option: Optional variable-length fields, including packet type, valid lease time, IP address of a DNS server, and IP address of the WINS server.

DHCP Packet Processing Modes

After the DHCP server is enabled on a device, the device processes the DHCP packet received from a DHCP client in one of the following three modes depending on your configuration:

- Global address pool: In response to the DHCP packets received from DHCP clients, the DHCP server picks IP addresses from its global address pools and assigns them to the DHCP clients.
- Interface address pool: In response to the DHCP packets received from DHCP clients, the DHCP server picks IP addresses from the interface address pools and assigns them to the DHCP clients. If there is no available IP address in the interface address pools, the DHCP server picks IP addresses from its global address pool that contains the interface address pool segment and assigns them to the DHCP clients.
- Trunk: DHCP packets received from DHCP clients are forwarded to an external DHCP server, which assigns IP addresses to the DHCP clients.

You can specify the mode to process DHCP packets. For the configuration of the first two modes, see Chapter 57 "DHCP Server Configuration" on page 593. For the configuration of the trunk mode, see Chapter 58 "DHCP Relay Agent Configuration" on page 611.

One interface only corresponds to one mode. In this case, the new configuration overwrites the previous one.

Protocols and Standards

Protocol specifications related to DHCP include:

- RFC2131: Dynamic Host Configuration Protocol
- RFC2132: DHCP Options and BOOTP Vendor Extensions
- RFC1542: Clarifications and Extensions for the Bootstrap Protocol

57 DHCP SERVER CONFIGURATION

Introduction to DHCP Server

Usage of DHCP Server

Generally, DHCP servers are used in the following networks to assign IP addresses:

- Large-sized networks, where manual configuration method bears heavy load and is difficult to manage the whole network in a centralized way.
- Networks where the number of available IP addresses is less than that of the hosts. In this type of networks, IP addresses are not enough for all the hosts to obtain a fixed IP address, and the number of on-line users is limited (such is the case in an ISP network). In these networks, a great number of hosts must dynamically obtain IP addresses through DHCP.
- Networks where only a few hosts need fixed IP addresses and most hosts do not need fixed IP addresses.

DHCP Address Pool

A DHCP address pool holds the IP addresses to be assigned to DHCP clients. When a DHCP server receives a DHCP request from a DHCP client, it selects an address pool depending on the configuration, picks an IP address from the pool and sends the IP address and other related parameters (such as the IP address of the DNS server, and the lease time of the IP address) to the DHCP client.

Types of address pools

The address pools of a DHCP server fall into two types: global address pool and interface address pool.

- A global address pool is created by executing the **dhcp server ip-pool** command in system view. It is valid on the current device.
- If an interface is configured with a valid unicast IP address, you can create an interface-based address pool for the interface by executing the **dhcp select interface** command in interface view. The IP addresses an interface address pool holds belong to the network segment the interface resides in and are available to the interface only.

The structure of an address pool

The address pools of a DHCP server are hierarchically organized in a tree-like structure. The root holds the IP addresses of the network segment, the branches hold the subnet IP addresses, and the leaves hold the IP addresses that are manually bound to specific clients. The address pools that are of the same level are sorted by their configuration precedence order. Such a structure enables configurations to be inherited. That is, the configurations of the network segment can be inherited by its subnets, whose configurations in turn can be inherited by their client address. So, for the parameters that are common to the whole network

segment or some subnets (such as domain name), you just need to configure them on the network segment or the corresponding subnets. The following is the details of configuration inheritance.

1. A newly created child address pool inherits the configurations of its parent address pool.
2. For an existing parent-child address pool pair, when you perform a new configuration on the parent address pool:
   - The child address pool inherits the new configuration if there is no corresponding configuration on the child address pool.
   - The child address pool does not inherit the new configuration if there is already a corresponding configuration on the child address pool.

DHCP IP Address Preferences

Interfaces of the DHCP server can work in the global address pool mode or in the interface address pool mode. If the DHCP server works in the interface address pool mode, it picks IP addresses from the interface address pools and assigns them to the DHCP clients. If there is no available IP address in the interface address pools, the DHCP server picks IP addresses from its global address pool that contains the interface address pool segment and assigns them to the DHCP clients.

A DHCP server assigns IP addresses in interface address pools or global address pools to DHCP clients in the following sequence:

- IP addresses that are statically bound to the MAC addresses of DHCP clients
- IP addresses that are ever used by DHCP clients. That is, those in the assigned leases recorded by the DHCP server. If there is no record in the leases and the DHCP-DISCOVER packets sent by DHCP clients contain option 50 fields, the DHCP server assigns the IP address requested by option 50.
- The first IP address found among the available IP addresses in the DHCP address pool.
- If no IP address is available, the DHCP server queries lease-expired and conflicted IP addresses. If the DHCP server finds such IP addresses, it assigns them; otherwise the DHCP server does not assign IP addresses.

Global Address Pool-Based DHCP Server Configuration

Configuration Tasks

Table 461 Global address pool-based DHCP server configuration tasks

Configuration task	Description	Related section
Enable DHCP	Required	"Enabling DHCP" on page 595
Configure global address pool mode on interface(s)	Optional	"Configuring Global Address Pool Mode on Interface(s)" on page 595

Table 461 Global address pool-based DHCP server configuration tasks

Configuration task		Description	Related section
Configure how to assign IP addresses in a global address pool	Configure to assign IP addresses by static binding	One among these two options is required. Only one mode can be selected for the same global address pool.	"Configuring How to Assign IP Addresses in a Global Address Pool" on page 596
	Configure to assign IP addresses dynamically		
Configure DNS services for the DHCP server		Optional	"Configuring DNS Services for the DHCP Server" on page 597
Configure NetBIOS services for the DHCP server		Optional	"Configuring NetBIOS Services for the DHCP Server" on page 598
Customize DHCP service		Optional	"Customizing DHCP Service" on page 599
Configure gateway addresses for DHCP clients		Optional	"Configuring Gateway Addresses for DHCP Clients" on page 599

Enabling DHCP

You need to enable DHCP before performing other DHCP-related configurations, which takes effect only after DHCP is enabled.

Table 462 Enable DHCP

Operation	Command	Description
Enter system view	**system-view**	-
Enable DHCP	**dhcp enable**	Required By default, DHCP is enabled

Configuring Global Address Pool Mode on Interface(s)

You can configure the global address pool mode on the specified or all interfaces of a DHCP server. After that, when the DHCP server receives DHCP packets from DHCP clients through these interfaces, it assigns IP addresses in the global address pool to the DHCP clients.

Table 463 Configure the global address pool mode on interface(s)

Operation		Command	Description
Enter system view		**system-view**	-
Configure the specified interface(s) or all interfaces to operate in global address pool mode	Configure the current interface	**interface** *interface-type interface-number*	Optional By default, a DHCP server assigns the IP addresses of the global address pool to DHCP clients in response to DHCP packets received from DHCP clients
		dhcp select global	
		quit	
	Configure multiple interfaces in system view	**dhcp select global** { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	

Configuring How to Assign IP Addresses in a Global Address Pool

You can specify to bind an IP address in a global address pool statically to a DHCP client or assign IP addresses in the pool dynamically to DHCP clients as needed. In the global address pool, you can bind an IP address statically to a DHCP client and assign other IP addresses in the pool dynamically to DHCP clients.

For dynamic IP address assigning, you need to specify the range of the IP addresses to be dynamically assigned. But for static IP address binding, you can consider an IP address statically bound to a DHCP client coming from a special DHCP address pool that contains only one IP address.

Configuring to assign IP addresses by static binding

Some DHCP clients, such as WWW servers, need fixed IP addresses. This can be achieved by binding IP addresses to the MAC addresses of these DHCP clients. When such a DHCP client applies for an IP address, the DHCP server searches for the IP address corresponding to the MAC address of the DHCP client and assigns the IP address to the DHCP client.

Currently, only one IP address in a global DHCP address pool can be statically bound to a MAC address.

Table 464 Configure to assign IP addresses by static binding

Operation	Command	Description
Enter system view	**system-view**	-
Create a DHCP address pool and enter DHCP address pool view	**dhcp server ip-pool** *pool-name*	Required By default, no global DHCP address pool is created
Configure an IP address to be statically bound	**static-bind ip-address** *ip-address* [**mask** *mask*]	Required By default, no IP address is statically bound
Configure a client MAC address to which an IP address is to be statically bound	**static-bind mac-address** *mac-address*	Required By default, no MAC address to which an IP address is to be statically bound is configured



- *The **static-bind ip-address** command and the **static-bind mac-address** command must be coupled.*
- *In the same global DHCP address pool, if the **static-bind ip-address** command or the **static-bind mac-address** command is executed repeatedly, the new configuration overwrites the previous one.*
- *The IP address to be statically bound cannot be an interface IP address of the DHCP server; otherwise static binding does not take effect.*
- *A client can permanently use the statically-bound IP address that it has obtained. The IP address is not limited by the lease time of the IP addresses in the address pool.*

Configuring to assign IP addresses dynamically

IP addresses dynamically assigned to DHCP clients (including those that are permanently leased and those that are temporarily leased) belong to addresses segments that are previously specified. Currently, an address pool can contain only one address segment, whose ranges are determined by the subnet mask.

To avoid IP address conflicts, the IP addresses to be dynamically assigned to DHCP clients are those that are not occupied by specific network devices (such as gateways and FTP servers).

The lease time can differ with address pools. But that of the IP addresses of the same address pool are the same. Lease time is not inherited, that is to say, the lease time of a child address pool is not affected by the configuration of the parent address pool.

Table 465 Configure to assign IP addresses dynamically

Operation	Command	Description
Enter system view	**system-view**	-
Create a DHCP address pool and enter DHCP address pool view	**dhcp server ip-pool** *pool-name*	Required By default, no DHCP address pool is created
Set the IP address segment whose IP addresses are to be assigned dynamically	**network** *ip-address* [**mask** *mask*]	Required By default, no IP address segment is set. That is, no IP address is available for being assigned
Configure the lease time	**expired** { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }	Optional The default lease time is one day
Return to system view	**quit**	-
Specify the IP addresses that are not dynamically assigned	**dhcp server forbidden-ip** *low-ip-address* [*high-ip-address*]	Optional By default, all IP addresses in a DHCP address pool are available for being dynamically assigned



- *In the same DHCP global address pool, the **network** command can be executed repeatedly. In this case, the new configuration overwrites the previous one.*
- *The **dhcp server forbidden-ip** command can be executed repeatedly. That is, you can repeatedly configure IP addresses that are not dynamically assigned to DHCP clients.*

Configuring DNS Services for the DHCP Server

If a host accesses the Internet through domain names, DNS is needed to translate the domain names into the corresponding IP addresses. To enable DHCP clients to access the Internet through domain names, a DHCP server is required to provide DNS server addresses while assigning IP addresses to DHCP clients. Currently, you can configure up to eight DNS server addresses for a DHCP address pool.

You can configure domain names to be used by DHCP clients for address pools. After you do this, the DHCP server provides the domain names to the DHCP clients as well while the former assigns IP addresses to the DHCP clients.

Table 466 Configure DNS services for the DHCP server

Operation	Command	Description
Enter system view	**system-view**	-

Table 466 Configure DNS services for the DHCP server

Operation	Command	Description
Create a DHCP address pool and enter DHCP address pool view	**dhcp server ip-pool** *pool-name*	Required By default, no global DHCP address pool is created
Configure a domain name for DHCP clients	**domain-name** *domain-name*	Required By default, no domain name is configured for DHCP clients
Configure DNS server addresses for DHCP clients	**dns-list** *ip-address*&<1-8>	Required By default, no DNS server address is configured

Configuring NetBIOS Services for the DHCP Server

For Microsoft Windows-based DHCP clients that communicate through NetBIOS protocol, the host name-to-IP address translation is carried out by Windows internet naming service (WINS) servers. So you need to perform WINS-related configuration for most Windows-based hosts. Currently, you can configure up to eight WINS addresses for a DHCP address pool.

Host name-to-IP address mappings are needed for DHCP clients communicating through NetBIOS protocol. According to the way to establish the mapping, NetBIOS nodes fall into the following four categories:

- B-node. Nodes of this type establish their mappings through broadcasting (The character b stands for the word broadcast). The source node obtains the IP address of the destination node by sending the broadcast packet containing the host name of the destination node. After receiving the broadcast packet, the destination node returns its IP address to the source node.
- P-node. Nodes of this type establish their mappings by sending unicast packets to WINS servers. (The character p stands for peer-to-peer). The source node sends the unicast packet to the WINS server. After receiving the unicast packet, the WINS server returns the IP address corresponding to the destination node name to the source node.
- M-node. Nodes of this type are p-nodes mixed with broadcasting features (The character m stands for the word mixed), that is to say, this type of nodes obtain mappings by sending broadcast packets first. If they fail to obtain mappings, they send unicast packets to the WINS server to obtain mappings.
- H-node. Nodes of this type are b-nodes mixed with peer-to-peer features. (The character h stands for the word hybrid), that is to say, this type of nodes obtain mappings by sending unicast packets to WINS servers. If they fail to obtain mappings, they send broadcast packets to obtain mappings.

Table 467 Configure NetBIOS services for the DHCP server

Operation	Command	Description
Enter system view	**system-view**	-
Create a DHCP address pool and enter DHCP address pool view	**dhcp server ip-pool** *pool-name*	Required By default, no global DHCP address pool is created

Table 467 Configure NetBIOS services for the DHCP server

Operation	Command	Description
Configure WINS server addresses for DHCP clients	**nbns-list** *ip-address*&<1-8>	Required By default, no WINS server address is configured
Configure DHCP clients to be of a specific NetBIOS node type	**netbios-type** { **b-node** | **h-node** | **m-node** | **p-node** }	Optional By default, no NetBIOS node type of the DHCP client is specified and a DHCP client uses an h-node

Customizing DHCP Service

With the evolution of DHCP, new options are constantly coming into being. You can add the new options as the properties of DHCP servers by performing the following configuration.

Table 468 Customize DHCP service

Operation	Command	Description
Enter system view	**system-view**	-
Create a DHCP address pool and enter DHCP address pool view	**dhcp server ip-pool** *pool-name*	Required By default, no global DHCP address pool is created
Configure customized options	**option** *code* { **ascii** *ascii-string* | **hex** *hex-string*&<1-10> | **ip-address** *ip-address*&<1-8> }	Required By default, no customized option is configured

Configuring Gateway Addresses for DHCP Clients

Gateways are necessary for DHCP clients to access servers/hosts outside the current network segment. After you configure gateway addresses on a DHCP server, the DHCP server provides the gateway addresses to DHCP clients as well while assigning IP addresses to them.

You can configure gateway addresses for address pools on a DHCP server. Currently, you can configure up to eight gateway addresses for a DHCP address pool.

Table 469 Configure gateway addresses for DHCP clients

Operation	Command	Description
Enter system view	**system-view**	-
Create a DHCP address pool and enter DHCP address pool view	**dhcp server ip-pool** *pool-name*	Required By default, no global DHCP address pool is created
Configure gateway addresses for DHCP clients	**gateway-list** *ip-address*&<1-8>	Required By default, no gateway address is configured

Interface Address Pool-Based DHCP Server Configuration



CAUTION: *In the interface address pool mode, after the addresses in the interface address pool have been assigned, the DHCP server picks IP addresses from the global interface address pool containing the segment of the interface address pool and assigns them to the DHCP clients. As a result, the IP addresses obtained from global address pools and those obtained from interface address pools are not in the same network segment, so the clients cannot interoperate with each other.*

In the interface address pool mode, if the IP addresses in the same address pool are required to be assigned to the clients on the same VLAN interface, the number of clients that obtain IP addresses automatically cannot exceed the number of the IP addresses that can be assigned in the interface address pool.

Configuration Overview

An interface address pool is created when the interface is assigned a valid unicast IP address and you execute the **dhcp select interface** command in interface view. The IP addresses contained in it belong to the network segment where the interface resides and are available to the interface only.

You can perform certain configurations for DHCP address pools of an interface or multiple interfaces within specified interface ranges. Configuring for multiple interfaces eases configuration work load and makes you to configure in a more convenient way.

Table 470 Interface address pool-based DHCP server configuration tasks

Configuration task		Description	Related section
Enable DHCP		Required	"Enabling DHCP" on page 601
Configure to assign the IP addresses of interface address pools to DHCP clients		Required	"Configuring to Assign the IP Addresses of Interface Address Pools to DHCP Clients" on page 601
Configure to assign IP addresses of DHCP address pools to DHCP clients	Configure to assign IP addresses by static binding	One among these two options is required. These two options can be configured at the same time.	"Configuring to Assign IP Addresses of DHCP Address Pools to DHCP Clients" on page 601
	Configure to assign IP addresses dynamically		
Configure DNS services for the DHCP server		Optional	"Configuring DNS Services for the DHCP Server" on page 603
Configure NetBIOS services for DHCP clients		Optional	"Configuring NetBIOS Services for DHCP Clients" on page 604

Table 470 Interface address pool-based DHCP server configuration tasks

Configuration task	Description	Related section
Customize DHCP service	Optional	"Customizing DHCP Service" on page 605

Enabling DHCP

You need to enable DHCP before performing DHCP configurations. DHCP-related configurations are valid only when DHCP is enabled.

Table 471 Enable DHCP

Operation	Command	Description
Enter system view	**system-view**	-
Enable DHCP	**dhcp enable**	Required By default, DHCP is enabled

Configuring to Assign the IP Addresses of Interface Address Pools to DHCP Clients

If the DHCP server works in the interface address pool mode, it picks IP addresses from the interface address pools and assigns them to the DHCP clients. If there is no available IP address in the interface address pools, the DHCP server picks IP addresses from its global address pool that contains the interface address pool segment and assigns them to the DHCP clients.

Table 472 Configure to assign the IP addresses of interface address pools to DHCP clients

Operation		Command	Description
Enter system view		**system-view**	-
Configure to assign the IP addresses of interface address pools to DHCP clients	Configure the current interface	**interface** *interface-type interface-number*	Required By default, a DHCP server assigns the IP addresses of the global address pool to DHCP clients
		dhcp select interface	
		quit	
	Configure multiple interfaces in system view	**dhcp select interface** { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	

Configuring to Assign IP Addresses of DHCP Address Pools to DHCP Clients

You can assign IP addresses by static binding or assign IP addresses dynamically to DHCP clients as needed.

Configuring to assign IP addresses by static binding

Some DHCP clients, such as WWW servers, need fixed IP addresses. This is achieved by binding IP addresses to the MAC addresses of these DHCP clients. When such a DHCP client applies for an IP address, the DHCP server finds the IP address corresponding to the MAC address of the DHCP client, and then assigns the IP address to the DHCP client.

Table 473 Configure to assign IP addresses by static binding

Operation	Command	Description
Enter system view	**system-view**	-

Table 473 Configure to assign IP addresses by static binding

Operation	Command	Description
Enter interface view	**interface** *interface-type interface-number*	-
Configure static binding	**dhcp server static-bind ip-address** *ip-address* **mac-address** *mac-address*	Required By default, static binding is not configured



- *There is no limit to the number of IP addresses statically bound in an interface address pool, but the IP addresses statically bound in interface address pools and the interface IP addresses must be in the same segment.*
- *An IP address can be statically bound to only one MAC address. A MAC address can be bound with only one IP address statically.*
- *The IP address to be statically bound cannot be an interface IP address of the DHCP server; otherwise the static binding does not take effect.*

Configuring to assign IP addresses dynamically

As an interface-based address pool is created after the interface is assigned a valid unicast IP address, the IP addresses contained in the address pool belong to the network segment where the interface resides and are available to the interface only. So specifying the range of the IP addresses to be dynamically assigned is unnecessary.

To avoid IP address conflicts, the IP addresses to be dynamically assigned to DHCP clients are those not occupied by specific network devices (such as gateways and FTP servers).

The lease time can differ with address pools. But that of the IP addresses of the same address pool is the same. Lease time is not inherited, that is to say, the lease time of a child address pool is not affected by the configuration of the parent address pool.

Table 474 Configure to assign IP addresses dynamically

Operation		Command	Description
Enter system view		**system-view**	-
Configure the lease time	Configure for the current interface	**interface** *interface-type interface-number*	Optional The default lease time is one day
		dhcp server expired { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }	
		quit	
	Configure multiple interfaces in system view	**dhcp server expired** { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** } { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	

Table 474 Configure to assign IP addresses dynamically

Operation	Command	Description
Specify the IP addresses that are not dynamically assigned	**dhcp server forbidden-ip** *low-ip-address* [*high-ip-address*]	Optional By default, all IP addresses in a DHCP address pool are available for being dynamically assigned.

- *The **dhcp server forbidden-ip** command can be executed repeatedly. That is, you can repeatedly configure IP addresses that are not dynamically assigned to DHCP clients.*
- *Use the **dhcp server forbidden-ip** command to configure the IP addresses that are not assigned dynamically in global address pools and interface address pools.*

Configuring DNS Services for the DHCP Server

If a host accesses the Internet through domain names, DNS is needed to translate the domain names into the corresponding IP addresses. To enable DHCP clients to access the Internet through domain names, a DHCP server is required to provide DNS server addresses while assigning IP addresses to DHCP clients. Currently, you can configure up to eight DNS server addresses for a DHCP address pool.

On the DHCP server, you can configure domain names to be used by DHCP clients for address pools. After you do this, the DHCP server provides the domain names to the DHCP clients while the DHCP server assigns IP addresses to the DHCP clients.

Table 475 Configure DNS services for the DHCP server

Operation		Command	Description
Enter system view		**system-view**	-
Configure a domain name for DHCP clients	Configure the current interface	**interface** *interface-type interface-number*	Required By default, no domain name is configured for DHCP clients
		dhcp server domain-name *domain-name*	
		quit	
	Configure multiple interfaces in system view	**dhcp server domain-name** *domain-name* { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	

Table 475 Configure DNS services for the DHCP server

Operation		Command	Description
Configure DNS server addresses for DHCP clients	Configure the current interface	**interface** *interface-type interface-number*	Required By default, no DNS server address is configured.
		dhcp server dns-list *ip-address*&<1-8>	
		quit	
	Configure multiple interfaces in system view	**dhcp server dns-list** *ip-address*&<1-8> { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	

Configuring NetBIOS Services for DHCP Clients

For Microsoft Windows-based DHCP clients that communicate through NetBIOS protocol, the host name-to-IP address translation is carried out by WINS servers. So you need to perform WINS-related configuration for most Windows-based hosts. Currently, you can configure up to eight WINS addresses for a DHCP address pool.

Host name-to-IP address mappings are needed for DHCP clients communicating through the NetBIOS protocol. According to the way to establish the mapping, NetBIOS nodes fall into the following four categories:

- B-node. Nodes of this type establish their mappings through broadcasting (The character b stands for the word broadcast). The source node obtains the IP address of the destination node by sending the broadcast packet containing the host name of the destination node. After receiving the broadcast packet, the destination node returns its IP address to the source node.
- P-node. Nodes of this type establish their mappings by communicating with WINS servers (The character p stands for peer-to-peer). The source node sends the unicast packet to the WINS server. After receiving the unicast packet, the WINS server returns the IP address corresponding to the destination node name to the source node.
- M-node. Nodes of this type are p-nodes mixed with broadcasting features (The character m stands for the word mixed), that is to say, this type of nodes obtain mappings by sending broadcast packets first. If they fail to obtain mappings, they send unicast packets to the WINS server to obtain mappings.
- H-node. Nodes of this type are b-nodes mixed with peer-to-peer features (The character h stands for the word hybrid), that is to say, this type of nodes obtain mappings by sending unicast packets to WINS servers. If they fail to obtain mappings, they send broadcast packets to obtain mappings.

Table 476 Configure NetBIOS services for the DHCP server

Operation	Command	Description
Enter system view	**system-view**	-

Table 476 Configure NetBIOS services for the DHCP server

Operation		Command	Description
Configure the WINS server address for DHCP clients	Configure the current interface	**interface** *interface-type interface-number*	Required By default, no WINS server address is configured
		dhcp server nbns-list *ip-address*&<1-8>	
		quit	
	Configure multiple interfaces in system view	**dhcp server nbns-list** *ip-address*&<1-8> { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	
Configure NetBIOS node types for DHCP clients	Configure the current interface	**interface** *interface-type interface-number*	Required By default, no NetBIOS node type is specified and a DHCP client uses an h-node.
		dhcp server netbios-type { **b-node** | **h-node** | **m-node** | **p-node** }	
		quit	
	Configure multiple interfaces in system view	**dhcp server netbios-type** { **b-node** | **h-node** | **m-node** | **p-node** } { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	

Customizing DHCP Service

With the evolution of DHCP, new options are constantly coming into being. You can add the new options as the properties of DHCP servers by performing the following configuration.

Table 477 Customize DHCP service

Operation		Command	Description
Enter system view		**system-view**	-
Configure customized options	Configure the current interface	**interface** *interface-type interface-number*	Required By default, no customized option is configured
		dhcp server option *code* { **ascii** *ascii-string* | **hex** *hex-string*&<1-10> | **ip-address** *ip-address*&<1-8> }	
		quit	
	Configure multiple interfaces in system view	**dhcp server option** *code* { **ascii** *ascii-string* | **hex** *hex-string*&<1-10> | **ip-address** *ip-address*&<1-8> } { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	

DHCP Security Configuration

DHCP security configuration is needed to ensure the security of DHCP service.

Prerequisites

Before configuring DHCP security, you should first complete the DHCP server configuration (either global address pool-based or interface address pool-based DHCP server configuration).

Configuring Private DHCP Server Detecting

A private DHCP server on a network also answers IP address request packets and assigns IP addresses to DHCP clients. However, the IP addresses they assigned may conflict with those of other hosts. As a result, users cannot normally access networks. This kind of DHCP servers are known as private DHCP servers.

With the private DHCP server detecting function enabled, when a DHCP client sends the DHCP-REQUEST packet, the DHCP server tracks the information (such as the IP addresses and interfaces) of DHCP servers to enable the administrator to detect private DHCP servers in time and take proper measures.

Table 478 Enable detection of a private DHCP server

Operation	Command	Description
Enter system view	**system-view**	-
Enable the private DHCP server detecting function	**dhcp server detect**	Required By default, the private DHCP server detecting function is disabled

Configuring IP Address Detecting

To avoid IP address conflicts caused by assigning the same IP address to multiple DHCP clients simultaneously, you can configure a DHCP server to detect an IP address before it assigns the address to a DHCP client.

IP address detecting is achieved by performing ping operations. To detect whether an IP address is currently in use, the DHCP server sends an ICMP packet with the IP address to be assigned as the destination and waits for a response. If the DHCP server receives no response within a specified time, it resends an ICMP packet. This procedure repeats until the DHCP server receives a response or the number of the sent ICMP packets reaches the specified maximum number. The DHCP server assigns the IP address to the DHCP client only when no response is received during the whole course, thus ensuring that an IP address is assigned to one DHCP client exclusively.

Table 479 Configure IP address detecting

Operation	Command	Description
Enter system view	**system-view**	-
Set the maximum number of ICMP packets a DHCP server sends in a ping test	**dhcp server ping packets** *number*	Optional By default, a DHCP server performs the ping operation twice to test an IP address
Set the response timeout time of each ICMP packet	**dhcp server ping timeout** *milliseconds*	Optional The default timeout time is 500 milliseconds

Displaying and Maintaining a DHCP Server

After the above configuration, execute the **display** command in any view to display and verify the DHCP server configuration.

Execute the **reset** command in user view to clear DHCP server configuration information.

Table 480 Display and maintain DHCP server configuration

Operation	Command	Description
Display the statistics on IP address conflicts	**display dhcp server conflict** { **all** | **ip** *ip-address* }	You can execute the **display** command in any view.
Display lease expiration information	**display dhcp server expired** { **ip** *ip-address* | **pool** [*pool-name*] | **interface** [*interface-type interface-number*] **all** }	
Display the free IP addresses	**display dhcp server free-ip**	
Display information about address binding	**display dhcp server ip-in-use** { **ip** *ip-address* | **pool** [*pool-name*] | **interface** [*interface-type interface-number*] **all** }	
Display the statistics on a DHCP server	**display dhcp server statistics**	
Display information about DHCP address pool tree	**display dhcp server tree** { **pool** [*pool-name*] | **interface** [*interface-type interface-number*] | **all** }	
Clear IP address conflict statistics	**reset dhcp server conflict** { **all** | **ip** *ip-address* }	You can execute the **reset** command in user view.
Clear dynamic address binding information	**reset dhcp server ip-in-use** { **ip** *ip-address* | **pool** [*pool-name*] | **interface** [*interface-type interface-number*] | **all** }	
Clear the statistics on a DHCP server	**reset dhcp server statistics**	

*Executing the **save** command will not save the lease information on a DHCP server to the flash memory. Therefore, the configuration file contains no lease information after the DHCP server restarts or you clear the lease information by executing the **reset dhcp server ip-in-use** command. In this case, any lease-update requests will be denied, and the clients must apply for IP addresses again.*

DHCP Server Configuration Example

Currently, DHCP networking can be implemented in two ways. One is to deploy the DHCP server and DHCP clients in the same network segment. This enables the clients to communicate with the server directly. The other is to deploy the DHCP server and DHCP clients in different network segments. In this case, IP address assigning is carried out through DHCP relay agent. Note that DHCP server configuration is the same in both scenarios.

Network requirements

The DHCP server assigns IP addresses dynamically to the DHCP clients on the same network segment. The network segment 10.1.1.0/24, to which the IP addresses of the address pool belong, is divided into two sub-network segments: 10.1.1.0/25 and 10.1.1.128/25. The switch operating as the DHCP server hosts two VLANs, whose interface IP addresses are 10.1.1.1/25 and 10.1.1.129/25 respectively.

The DHCP settings of the 10.1.1.0/25 network segment are as follows:

- Lease time: 10 days plus 12 hours
- Domain name: aabbcc.com
- DNS server: 10.1.1.2
- WINS server: none
- Gateway: 10.1.1.126

The DHCP settings of the 10.1.1.128/25 network segment are as follows:

- Lease time: 5 days
- Domain name: aabbcc.com
- DNS server: 10.1.1.2
- WINS server: 10.1.1.4
- Gateway: 10.1.1.254

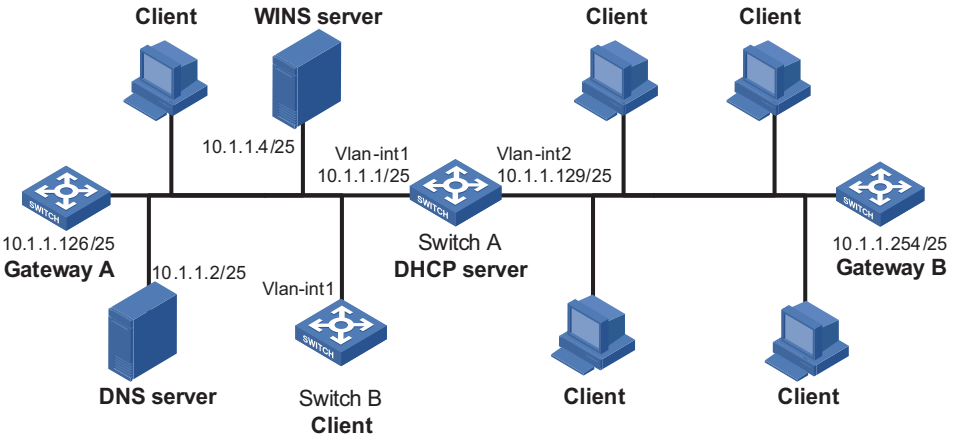
If you use the inheriting relation of parent and child address pools, make sure that the number of the assigned IP addresses does not exceed the number of the IP addresses in the child address pool; otherwise extra IP addresses will be obtained from the parent address pool. The attributes (for example, gateway) also are based on the configuration of the parent address pool.

For example, in the network to which VLAN-interface 1 is connected, if multiple clients apply for IP addresses, the child address pool 10.1.1.0/25 assigns IP addresses first. When the IP addresses in the child address pool have been assigned, if other clients need IP addresses, the IP addresses will be assigned from the parent address pool 10.1.1.0/24 and the attributes will be based on the configuration of the parent address pool.

For this example, the number of clients applying for IP addresses from VLAN-interface 1 is recommended to be less than or equal to 122 and the number of clients applying for IP addresses from VLAN-interface 2 is recommended to be less than or equal to 124.

Network diagram

Figure 154 Network diagram for DHCP configuration



Configuration procedure

1 Configure a VLAN and add a port in this VLAN, and then configure the IP address of the VLAN interface (omitted).

2 Configure DHCP service.

Enable DHCP.

```
<SW7750> system-view
[SW7750] dhcp enable
```

Configure the IP addresses that are not dynamically assigned. (That is, the IP addresses of the DNS server, WINS server, and gateways.)

```
[SW7750] dhcp server forbidden-ip 10.1.1.2
[SW7750] dhcp server forbidden-ip 10.1.1.4
[SW7750] dhcp server forbidden-ip 10.1.1.126
[SW7750] dhcp server forbidden-ip 10.1.1.254
```

Configure DHCP address pool 0, including address range and DNS server address.

```
[SW7750] dhcp server ip-pool 0
[SW7750-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
[SW7750-dhcp-pool-0] domain-name aabbcc.com
[SW7750-dhcp-pool-0] dns-list 10.1.1.2
[SW7750-dhcp-pool-0] quit
```

Configure DHCP address pool 1, including address range, gateway, and lease time.

```
[SW7750] dhcp server ip-pool 1
[SW7750-dhcp-pool-1] network 10.1.1.0 mask 255.255.255.128
[SW7750-dhcp-pool-1] gateway-list 10.1.1.126
[SW7750-dhcp-pool-1] expired day 10 hour 12
[SW7750-dhcp-pool-1] quit
```

Configure DHCP address pool 2, including address range, gateway, WINS server address, and lease time.

```
[SW7750] dhcp server ip-pool 2
[SW7750-dhcp-pool-2] network 10.1.1.128 mask 255.255.255.128
[SW7750-dhcp-pool-2] expired day 5
[SW7750-dhcp-pool-2] nbns-list 10.1.1.4
[SW7750-dhcp-pool-2] gateway-list 10.1.1.254
```

Troubleshooting a DHCP Server

Symptom

The IP address dynamically assigned by a DHCP server to a client conflicts with the IP address of another host.

Analysis

With DHCP enabled, IP address conflicts are usually caused by IP addresses that are manually configured on hosts.

Solution

- Disconnect the DHCP client from the network and then check whether there is a host using the conflicting IP address by performing ping operation on another host on the network, with the conflicting IP address as the destination and an enough timeout time.
- The IP address is manually configured on a host if you receive a response packet of the ping operation. You can then disable the IP address from being dynamically assigned by using the **dhcp server forbidden-ip** command on the DHCP server.
- Attach the DHCP client to the network, release the dynamically assigned IP address and obtain an IP address again. For example, enter DOS by executing the **cmd** command in Windows XP, and then release the IP address by executing the **ipconfig/release** command. Then obtain an IP address again by executing the **ipconfig/renew** command.

58 DHCP Relay Agent Configuration

Introduction to DHCP Relay Agent

Usage of DHCP Relay Agent

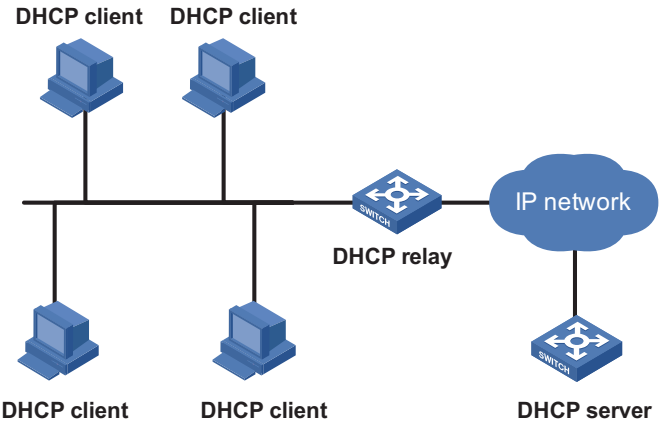
Since the packets are broadcasted in the process of obtaining IP addresses, DHCP is only applicable to the situation that DHCP clients and DHCP servers are in the same network segment, that is, you need to deploy at least one DHCP server for each network segment, which is far from economical.

The DHCP relay agent is designed to address this problem. It enables DHCP clients in a subnet to communicate with the DHCP server in another subnet so that the DHCP clients can obtain IP addresses. In this case, the DHCP clients in multiple networks can use the same DHCP server, which can decrease your cost and provide a centralized administration.

DHCP Relay Agent Fundamentals

Figure 155 illustrates a typical DHCP relay agent application.

Figure 155 Typical DHCP relay agent application



DHCP relay agents can transparently transmit broadcast packets on DHCP clients or servers to the DHCP servers or clients in other network segments.

In the process of dynamic IP address assignment through the DHCP relay agent, the DHCP client and DHCP server interoperate with each other in a similar way as they do without the DHCP relay agent. The following sections only describe the

forwarding process of the DHCP relay agent. For the interaction process of the packets, see "Obtaining IP Addresses Dynamically" on page 590.

1. The DHCP client broadcasts the DHCP-DISCOVER packet.
2. After receiving the packets, the network device providing the DHCP relay agent function unicasts the packet to the designated DHCP server based on the configuration.
3. The DHCP server assigns IP addresses and transmits the configuration information to the clients through the DHCP relay agent so that the clients can be configured dynamically. The transmission mode depends on the flag field in the DHCP-DISCOVER packet. For details, see "DHCP Packet Format" on page 590.

Option 82 Support

Introduction to option 82 support

Option 82 is a relay agent information option in DHCP packets. When a request packet from a DHCP client travels through a DHCP relay agent on its way to the DHCP server, the DHCP relay agent adds option 82 into the request packet. Option 82 includes many sub-options, but the DHCP server supports only sub-option 1 and sub-option 2 at present. Sub-option 1 defines agent circuit ID (that is, Circuit ID) and sub-option 2 defines remote agent ID (that is, Remote ID).

Option 82 enables a DHCP server to track the address information of DHCP relay agents, through which and other proper software, you can achieve the DHCP assignment limitation and accounting functions.

Primary terminologies

- Option: A length-variable field in DHCP packets, carrying information such as part of the lease information and packet type. It includes at least one option and at most 255 options.
- Option 82: Also known as relay agent information option. This option is a part of the Option field in DHCP packet. According to RFC3046, option 82 lies before option 255 and after the other options. Option 82 includes at least one sub-option and at most 255 sub-options. Currently, the commonly used sub-options in option 82 are sub-option 1 and sub-option 2.
- Sub-option 1: A sub-option of option 82. Sub-option 1 represents the agent circuit ID, namely Circuit ID. It holds the port number and VLAN-ID of the switch port connected to the DHCP client, and is usually configured on the DHCP relay agent. Generally, sub-option 1 and sub-option 2 must be used together to identify information about a DHCP source.
- Sub-option 2: A sub-option of option 82. Sub-option 2 represents the remote agent ID, namely Remote ID. It holds the MAC address of the DHCP relay agent, and is usually configured on the DHCP relay agent. Generally, sub-option 1 and sub-option 2 must be used together to identify information about a DHCP source.

Related specification

The specifications concerning option 82 supporting are as follows:

RFC2131 Dynamic Host Configuration Protocol

RFC3046 DHCP Relay Agent Information Option

Mechanism of option 82 supporting on DHCP relay agent

The procedure for a DHCP client to obtain an IP address from a DHCP server through a DHCP relay agent is similar to that for the client to obtain an IP address from a DHCP server directly. The following are the mechanism of option 82 supporting on DHCP relay agent.

1. A DHCP client broadcasts a request packet when it initiates.
2. The DHCP relay agent on the local network receives the request packet, and then checks whether the packet contains option 82 and processes the packet accordingly.
3. If the packet contains option 82, the DHCP relay agent processes the packet depending on the configured policy (that is, discards the packet, replaces the original option 82 in the packet with its own, or leaves the original option 82 unchanged in the packet), and forwards the packet (if not discarded) to the DHCP server.
4. If the packet does not contain option 82, the DHCP relay agent adds option 82 to the packet and forwards the packet to the DHCP server. The forwarded packet contains the port number of the switch to which the DHCP client is connected, the VLAN to which the DHCP client belongs, and the MAC address of the DHCP relay agent.
5. Upon receiving the DHCP request packet forwarded by the DHCP relay agent, the DHCP server stores the information contained in the option field and sends a packet that contains DHCP configuration information and option 82 to the DHCP relay agent.
6. Upon receiving the packet returned from the DHCP server, the DHCP relay agent strips option 82 from the packet and forwards the packet with the DHCP configuration information to the DHCP client.



Request packets sent by a DHCP client fall into two categories: DHCP-DISCOVER packets and DHCP-REQUEST packets. As DHCP servers coming from different manufacturers process DHCP request packets in different ways (that is, some DHCP servers process option 82 in DHCP-DISCOVER packets, whereas the rest process option 82 in DHCP-REQUEST packets), a DHCP relay agent adds option 82 to both types of packets to accommodate to DHCP servers of different manufacturers.

Configuring DHCP Relay Agent

Introduction to DHCP Relay Agent Configuration Tasks

Table 481 DHCP relay agent configuration tasks

Configuration task	Description	Related section
Enable DHCP	Required	"Enabling DHCP" on page 614
Configure an interface to operate in DHCP relay agent mode	Required	"Configuring an Interface to Operate in DHCP Relay Agent Mode" on page 614

Table 481 DHCP relay agent configuration tasks

Configuration task	Description	Related section
Configure a DHCP relay agent to broadcast responses to clients	Optional	"Configuring a DHCP Relay Agent to Broadcast Responses to Clients" on page 615
Specify gateways for DHCP clients	Optional	"Specifying Gateways for DHCP Clients" on page 615
Specify source IP address of uplink packets	Optional	"Specifying the Source IP Address of Uplink Packets" on page 616
Configure DHCP relay agent security functions	Optional	"Configuring DHCP Relay Agent Security Functions" on page 617
Configure Option 82 support	Optional	"Configuring Option 82 Support" on page 619

Enabling DHCP

Make sure to enable DHCP before you perform other DHCP relay agent-related configurations, since other DHCP-related configurations cannot take effect with DHCP disabled.

Table 482 Enable DHCP

Operation	Command	Description
Enter system view	**system-view**	-
Enable DHCP	**dhcp enable**	Required By default, DHCP is enabled

Configuring an Interface to Operate in DHCP Relay Agent Mode

When an interface operates in the relay mode, the interface forwards the DHCP packets received from DHCP clients to an external DHCP server, which assigns IP addresses to the DHCP clients.

To enhance reliability, you can set multiple DHCP servers on the same network. These DHCP servers form a DHCP server group. When the interface establishes mapping relationship with the DHCP server group, the interface forwards the DHCP packets to all servers in the server group.

Table 483 Configure an interface to operate in DHCP relay agent mode

Operation	Command	Description
Enter system view	**system-view**	-
Configure the DHCP server IP address(es) in a specified DHCP server group	**dhcp-server** *groupNo* **ip** *ip-address*&<1-8>	Required By default, no DHCP server IP address is configured in a DHCP server group

Table 483 Configure an interface to operate in DHCP relay agent mode

Operation	Command	Description
Map an interface to a DHCP server group	**interface** *interface-type interface-number*	Required
	dhcp-server *groupNo*	By default, a VLAN interface is not mapped to any DHCP server group

- *You can configure up to eight external DHCP IP addresses in a DHCP server group.*
- *You can map multiple VLAN interfaces to one DHCP server group. But one VLAN interface can be mapped to only one DHCP server group. If you execute the* ***dhcp-server*** *groupNo command repeatedly, the new configuration overwrites the previous one.*
- *You need to configure the group number specified in the* ***dhcp-server*** *groupNo command in VLAN interface view by using the command* ***dhcp-server*** *groupNo* ***ip*** *ipaddress-address&<1-8> in advance.*

Configuring a DHCP Relay Agent to Broadcast Responses to Clients

Generally, the DHCP relay agent determines to broadcast or unicast responses (including DHCP-OFFER, DHCP-ACK, or DHCP-NAK) from the DHCP server to the clients according to the flag field in the DHCP-DISCOVER packet.

- When the first bit of the flag field is set to 1, the DHCP relay agent broadcasts the response packets to the clients.
- When the flag field is set to 0, the DHCP relay agent unicasts the response packets to the clients.

In actual networking, if clients have special requirements, Switch 7750 Ethernet switches support the following commands so as to force the DHCP relay agent to broadcast the responses to the clients. After this function is enabled, even if the flag field in the DHCP-DISCOVER packet is set to 0, the DHCP relay agent still broadcasts responses to the clients.

Table 484 Configure the DHCP relay agent to broadcast responses to clients

Operation	Command	Description
Enter system view	**system-view**	-
Configure the DHCP relay agent to broadcast responses to clients	**dhcp relay reply broadcast**	Required Generally, the DHCP relay agent determines to broadcast or unicast responses to the clients according to the flag field in the DHCP-DISCOVER packet.

Specifying Gateways for DHCP Clients

To implement this feature on the DHCP relay agent, you need to bind ports in a VLAN to either the VLAN interface's primary IP address or one of its secondary IP addresses (a gateway address). The binding entries will be stored in a binding table.

Upon receiving a DHCP request message with the giaddr field being 0 from a port in this VLAN, the DHCP relay agent will search the binding table and then insert the bound gateway IP address into the giaddr field of the message. If the DHCP relay agent cannot find a match in the binding table, it inserts the primary IP

address of the VLAN interface (connecting to the client) into the giaddr field of the message.

The DHCP server will assign an IP address in the same network segment as the gateway IP address to the client. Thus, clients connecting to different ports in a VLAN may get IP addresses in different network segments.

Specifying a gateway in Ethernet port view

Use the following commands to specify a gateway for the DHCP clients, that is, to bind a port in a VLAN to the VLAN interface's IP address (primary or secondary).

Table 485 Specify a gateway in Ethernet port view

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Bind the port in the specified VLAN to one of the VLAN interface's IP addresses (gateway)	**dhcp-relay gateway** *ip-address* **vlan** *vlan-id*	Required Not configured by default.

If the Ethernet port belongs to a sub-VLAN, you need to specify the ip address argument as the primary or secondary IP address of the corresponding super VLAN interface, and specify the vlan-id argument as the VLAN ID of the super VLAN; otherwise, the system prompts error information due to VLAN mismatch.

Specifying a gateway in VLAN interface view

Use the following commands to specify a gateway for the DHCP clients, that is, to bind ports in a VLAN to the VLAN interface's IP address (primary or secondary).

Table 486 Specify a gateway in VLAN interface view

Operation	Command	Description
Enter system view	**system-view**	-
Enter VLAN interface view	**interface vlan-interface** *vlan-id*	-
Bind multiple ports in the VLAN to one of the VLAN interface's IP addresses (gateway)	**dhcp-relay gateway** *ip-address* **interface** *interface-type interface-number* [**to** i*nterface-type interface-number*]	Required Not configured by default.

Removing all the gateways in system view

Table 487 Remove all the gateways in system view

Operation	Command	Description
Enter system view	**system-view**	-
Remove all the gateways	**undo dhcp-relay gateway all**	Required

Specifying the Source IP Address of Uplink Packets

When a Switch 7750 Ethernet switch working as a DHCP relay agent forwards a client's packet to the DHCP server, the source IP address of the packet is the IP address of the relay agent's interface that connects to the DHCP server by default.

However, if two equal-cost uplinks to the DHCP server exist, the packets from a client may have different source IP addresses. As a result, some packets may fail to pass the validity check.

Switch 7750 Ethernet switches supports specifying the source IP address of uplink packets. With this feature enabled on the relay agent, the source IP address of a client's packet to be forwarded to the DHCP server is the IP address of the receiving interface.

Table 488 Specify the source IP address of uplink packets

Operation	Command	Description
Enter system view	**system-view**	-
Specify the source IP address of packets on the DHCP relay agent	**dhcp relay source-ip source-interface**	Required This feature is disabled by default. That is, the source IP address of the packets sent to the DHCP server is the IP address of the relay agent's interface that connects to the DHCP server.

Configuring DHCP Relay Agent Security Functions

Configuring address checking

When a DHCP client obtains an IP address from a DHCP server through the DHCP relay agent, the DHCP relay agent automatically generates the binding between the client's IP address, MAC address, VLAN ID, and port number. You can also manually configure such bindings for clients on the DHCP relay agent.

The purpose of the address checking function on DHCP relay agent is to prevent unauthorized users from statically configuring IP addresses to access external networks. With this function enabled, a DHCP relay agent inhibits a user from accessing external networks if the binding of the IP address, MAC address, VLAN ID, and port number do not match any entries (including the entries dynamically tracked by the DHCP relay agent and the manually configured static entries) in the user address table on the DHCP relay agent.

Table 489 Configure address checking

Operation	Command	Description
Enter system view	**system-view**	-
Configure a static user address entry on the DHCP relay agent	**dhcp-security static** *ip-address* **mac** *mac-address* [**vlan** *vlan-id* | **port** *interface-type interface-number*]*	Optional By default, no DHCP user address entry is configured
Enter interface view	**interface** *interface-type interface-number*	-
Enable the address checking function	**address-check enable**	Required By default, the address checking function is disabled

Specifying address checking fields

After enabled with the address checking function, Switch 7750 Ethernet switches default to check the IP address, MAC address, VLAN ID, and port number of a DHCP client respectively. The DHCP client can access external networks only after an entry matching all the four fields is found in the client address table.

You can disable some fields (MAC address, VLAN ID, or port number) from address checking as needed. Thus, after enabled with address checking, the DHCP relay agent will not check the disabled fields, so that the clients not matching all the fields can also access external networks.

Table 490 Specify address checking fields

Operation	Command	Description
Enter system view	**system-view**	-
Enter interface view	**interface** *interface-type interface-number*	-
Specify address checking field(s)	**address-check field** { **mac | vlan | port** } **enable**	Optional By default, after enabled with the address checking function, the DHCP relay agent checks the IP address, MAC address, VLAN ID, and port number of a DHCP client respectively.
Disable specified address checking field(s)	**address-check field** { **mac | vlan | port** } **disable**	

*If you configure a static client address entry on the DHCP relay agent using the **dhcp-security static** command without specifying the **vlan** or **port** keyword, the DHCP relay agent will not check the VLAN ID or port number when performing address checking for the client, even if the two fields are enabled for address checking.*

Configuring dynamic entries

Through this configuration task, you can validate or invalidate the dynamic IP-to-MAC mapping entries generated by the DHCP relay agent. DHCP client addresses are matched based on the dynamic entries generated by DHCP relay agent only after these entries are activated; otherwise, DHCP client addresses are matched based only on the security address entries statically configured.

Table 491 Configure dynamic entries generated by DHCP relay agents

Operation	Command	Description
Enter system view	**system-view**	-
Enter VLAN interface view	**interface** *interface-type interface-number*	-
Validate the dynamic entries generated by the DHCP relay agent	**address-check dhcp-relay enable**	Optional By default, the dynamic IP-to-MAC mapping entries generated by the DHCP relay agent are valid

This configuration will take effect only after the address checking function of the DHCP relay agent on the VLAN interface is enabled.

Configuring whether to allow freely-connected clients to pass DHCP security check

A freely-connected client refers to the client whose IP address and MAC address are not in the DHCP security table. When the freely-connected client is not allowed to pass DHCP security check, you cannot access the network on this client even if the freely-connected client has a valid IP address.

Table 492 Configure whether to allow freely-connected clients to pass DHCP security check

Operation	Command	Description
Enter system view	**system-view**	-
Enter VLAN interface view	**interface** *interface-type interface-number*	-
Forbid freely-connected clients to pass DHCP security check	**address-check no-matched enable**	Optional Freely-connected clients are not allowed to pass DHCP security check

This configuration will take effect only after the address checking function of the DHCP relay agent on the VLAN interface is enabled.

Configuring Option 82 Support

Prerequisites

Before configuring option 82 supporting on a DHCP relay agent, you need to:

- Configure network parameters and relay function of the DHCP relay agent.
- Perform assignment strategy-related configurations, such as network parameters of the DHCP server, address pool, and lease time.
- The routes between the DHCP relay agent and the DHCP server are reachable.

Enabling option 82 supporting on a DHCP relay agent

The following operations need to be performed on a DHCP relay agent-enabled network device.

Table 493 Enable option 82 supporting on a DHCP relay agent

Operation	Command	Description
Enter system view	**system-view**	-
Enable option 82 supporting on the DHCP relay agent	**dhcp relay information enable**	Required By default, this function is disabled
Configure the strategy for the DHCP relay agent to process request packets containing option 82	**dhcp relay information strategy** { **drop** | **keep** | **replace** }	Optional By default, the **replace** policy is adopted



To enable option 82, you need to perform the corresponding configuration on the DHCP server and the DHCP relay agent.

Displaying and Maintaining DHCP Relay Agent

After the above configuration, execute the **display** command in any view to display and verify the DHCP relay agent configuration.

Execute the **reset** command in user view to clear the statistics information of the specified DHCP server group.

Table 494 Display DHCP relay agent configuration

Operation	Command	Description
Display the information about a specified DHCP server group	**display dhcp-server** *groupNo*	You can execute the **display** command in any view.
Display the information about the DHCP server group to which a specified VLAN interface is mapped	**display dhcp-server interface vlan-interface** *vlan-id*	
Display the address information of all the users in the valid user address table of the DHCP server group	**display dhcp-security** [*ip-address* | **dynamic** | **static**]	
Clear the statistics information of the specified DHCP server group	**reset dhcp-server** *groupNo*	You can execute the **reset** command in user view.

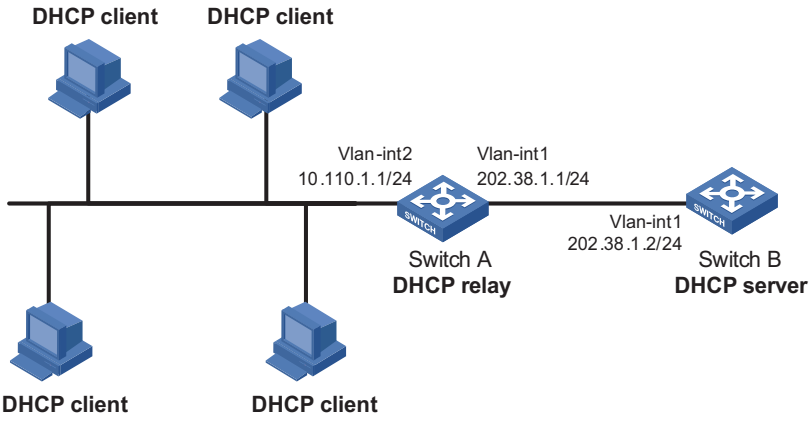
DHCP Relay Agent Configuration Example

Network requirements

The DHCP clients on the network segment 10.110.0.0/16 are connected to a port of VLAN 2. The IP address of the DHCP server is 202.38.1.2. DHCP packets between the DHCP clients and the DHCP server are forwarded by the DHCP relay agent, through which the DHCP clients can obtain IP addresses and related configuration information from the DHCP server.

Network diagram

Figure 156 Network diagram for DHCP relay agent



Configuration procedure

Enter system view.

```
<SW7750> system-view
```

Enable DHCP.

```
[SW7750] dhcp enable
```

Create DHCP server group 1 and configure an IP address of 202.38.1.2 for it.

```
[SW7750] dhcp-server 1 ip 202.38.1.2
```

Map VLAN-interface 2 to DHCP server group 1.

```
[SW7750] interface Vlan-interface 2
[SW7750-Vlan-interface2] dhcp-server 1
```

Configure an IP address for VLAN-interface 2, so that this interface is on the same network segment with the DHCP clients.

```
[SW7750-Vlan-interface2] ip address 10.110.1.1 255.255.0.0
```



You need to perform corresponding configurations on the DHCP server to enable the DHCP clients to obtain IP addresses from the DHCP server. The DHCP server configurations vary with different DHCP server devices, so the configurations are omitted.

Troubleshooting DHCP Relay Agent

Symptom

A client fails to obtain configuration information through a DHCP relay agent.

Analysis

This problem may be caused by improper DHCP relay agent configuration. When a DHCP relay agent operates improperly, you can locate the problem by enabling debugging and checking the information about debugging and interface state (You can display the information by executing the corresponding **display** command).

Solution

- Check if DHCP is enabled on the DHCP server and the DHCP relay agent.
- Check if an address pool that is on the same network segment with the DHCP clients is configured on the DHCP server.
- Check if a reachable route is configured between the DHCP relay agent and the DHCP server.
- Check the DHCP relay agent-enabled network devices. Check if the correct DHCP server group is configured on the interface connecting the network segment where the DHCP client resides. Check if the IP address of the DHCP server group is correct.

59 DHCP SNOOPING CONFIGURATION

Configuring DHCP Snooping

Introduction to DHCP Snooping

For the sake of security, the IP addresses used by online DHCP clients need to be tracked for the administrator to verify the corresponding relationship between the IP addresses the DHCP clients obtained from DHCP servers and the MAC addresses of the DHCP clients.

- Layer 3 switches can track DHCP client IP addresses through a DHCP relay agent.
- Layer 2 switches can track DHCP client IP addresses through the DHCP snooping function, which listens to DHCP broadcast packets.

When an unauthorized DHCP server exists in the network, a DHCP client may obtain an illegal IP address. To ensure that the DHCP clients obtain IP addresses from valid DHCP servers, you can specify a port to be a trusted port or an untrusted port through the DHCP snooping function.

- Trusted: A trusted port is connected to an authorized DHCP server directly or indirectly. It forwards DHCP messages to guarantee that DHCP clients can obtain valid IP addresses.
- Untrusted: An untrusted port is connected to an unauthorized DHCP server. The DHCP-ACK or DHCP-OFFER packets received from the port are discarded, preventing DHCP clients from receiving invalid IP addresses.

Figure 157 illustrates a typical network diagram for DHCP snooping application, where Switch A is a Switch 7750.

Figure 157 Typical network diagram for DHCP snooping application

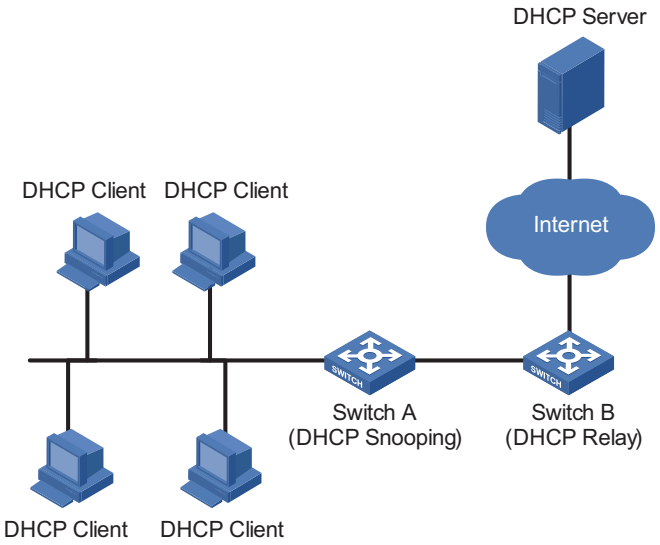
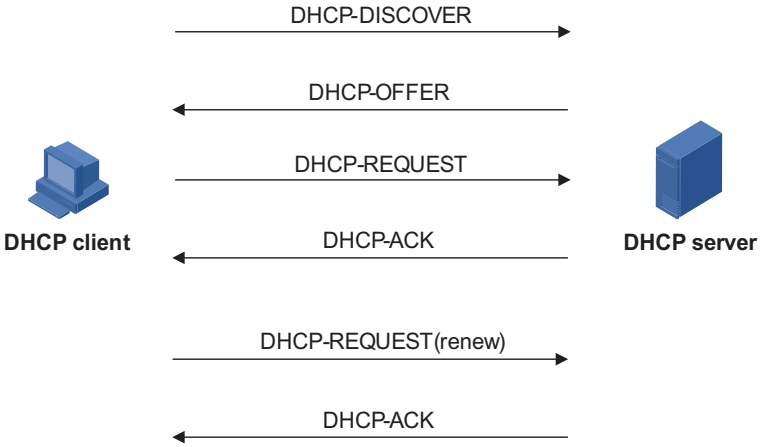


Figure 158 illustrates the interaction between a DHCP client and a DHCP server.

Figure 158 Interaction between a DHCP client and a DHCP server



DHCP snooping listens to the following two types of packets to retrieve the IP addresses the DHCP clients obtain from DHCP servers and the MAC addresses of the DHCP clients:

- DHCP-ACK packet
- DHCP-REQUEST packet

Introduction to DHCP-Snooping Option 82

Introduction to Option 82

For details about Option 82, refer to "Option 82 Support" on page 612.

Padding content and frame format of Option 82

There is no specification for what should be padded in Option 82. Manufacturers can pad it as required. By default, the sub-options of Option 82 for the Switch 7750 (enabled with DHCP snooping) are padded as follows:

- sub-option 1 (circuit ID sub-option): Padded with the port index (smaller than the physical port number by 1) and VLAN ID of the port that received the client's request.
- sub-option 2 (remote ID sub-option): Padded with the bridge MAC address of the DHCP snooping device that received the client's request.

By default, when Switch 7750s serve as DHCP snooping devices, Option 82 adopts the extended format. Refer to Figure 159 and Figure 160 for the extended format of the sub-options (with the default padding contents). That is, the circuit ID or remote ID sub-option defines the type and length of a circuit ID or remote ID.

The remote ID type field and circuit ID type field are determined by the option storage format. They are both set to **0** in the case of HEX format and to **1** in the case of ASCII format.

Figure 159 Extended format of the circuit ID sub-option

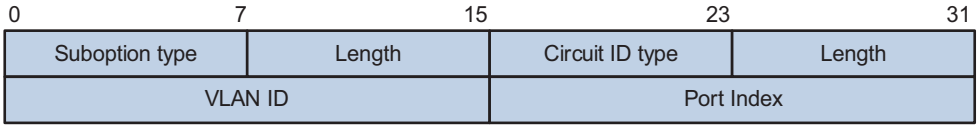
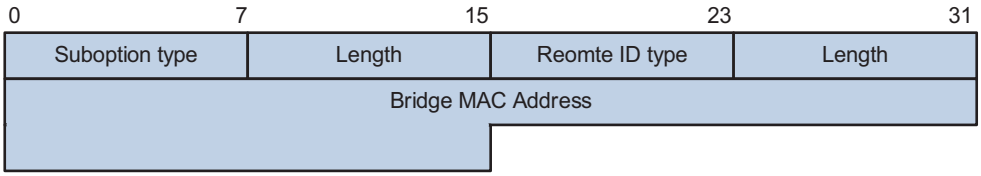


Figure 160 Extended format of the remote ID sub-option



In practice, some network devices do not support the type and length identifiers of the Circuit ID and Remote ID sub-options. To interwork with these devices, the Switch 7750 supports Option 82 in the standard format. Refer to Figure 161 and Figure 162 for the standard format of the sub-options (with the default padding contents). In the standard format, the Circuit ID or Remote ID sub-option does not contain the two-byte type and length fields of the circuit ID or remote ID.

Figure 161 Standard format of the circuit ID sub-option

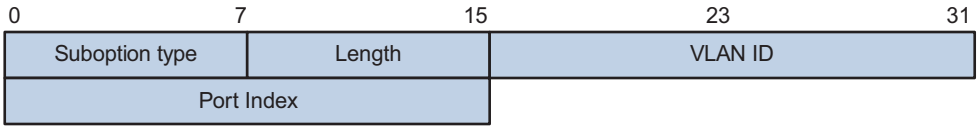
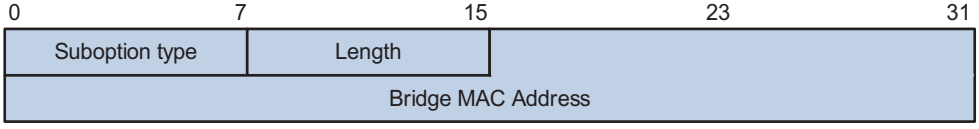


Figure 162 Standard format of the remote ID sub-option



Mechanism of DHCP-snooping Option 82

With DHCP snooping and DHCP-snooping Option 82 support enabled, when the DHCP snooping device receives a DHCP client's request containing Option 82, it will handle the packet according to the handling policy and the configured contents in sub-options. For details, see Table 495.

Table 495 Ways of handling a DHCP packet with Option 82

Handling policy	Sub-option configuration	The DHCP Snooping device will...
Drop	-	Drop the packet.
Keep	-	Forward the packet without changing Option 82.
Replace	Neither of the two sub-options is configured	Forward the packet after replacing the original Option 82 with the default content. The storage format of Option 82 content is the one specified with the **dhcp-snooping information format** command or the default HEX format if this command is not executed.
	Circuit ID sub-option is configured	Forward the packet after replacing the circuit ID sub-option of the original Option 82 with the configured circuit ID sub-option in ASCII format.
	Remote ID sub-option is configured	Forward the packet after replacing the remote ID sub-option of the original Option 82 with the configured remote ID sub-option in ASCII format.

When receiving a DHCP client's request without Option 82, the DHCP snooping device will add the option field with the configured sub-option and then forward the packet. For details, see Table 496.

Table 496 Ways of handling a DHCP packet without Option 82

Sub-option configuration	The DHCP-Snooping device will ...
Neither of the two sub-options is configured.	Forward the packet after adding Option 82 with the default contents. The format of Option 82 is the one specified with the **dhcp-snooping information format** command or the default HEX format if this command is not executed.
Circuit ID sub-option is configured.	Forward the packet after adding Option 82 with the configured circuit ID sub-option in ASCII format.
Remote ID sub-option is configured.	Forward the packet after adding Option 82 with the configured remote ID sub-option in ASCII format.

The circuit ID and remote ID sub-options in Option 82, which can be configured simultaneously or separately, are independent of each other in terms of configuration sequence.

Upon receiving a packet returned by the DHCP server, the DHCP snooping device checks the Option 82 field:

- If it was added by the local device, the device strips off Option 82 and forwards the packet to the DHCP client.
- If it was not added by the local device, the device obtains the VLAN information in Option 82 and broadcasts this packet within the VLAN.

There are two types of DHCP requests from DHCP clients, namely, DHCP_DISCOVER and DHCP_REQUEST messages. Since some DHCP servers process Option 82 in DHCP_DISCOVER messages while others process Option 82 in DHCP_DISCOVER messages, the DHCP snooping device will add Option 82 in both types of DHCP requests.

Introduction to IP Filtering

A denial-of-service (DoS) attack means an attempt of an attacker sending a large number of forged address requests with different source IP addresses to the server so that the network cannot work normally. The specific effects are as follows:

- The resources on the server are exhausted, so the server does not respond to other requests.
- After receiving such type of packets, a switch needs to send them to the CPU for processing. Too many request packets cause high CPU usage rate. As a result, the CPU cannot work normally.

The switch can filter invalid IP packets through the DHCP-snooping table and IP static binding table.

DHCP-snooping table

After DHCP snooping is enabled on a switch, a DHCP-snooping table is generated. It is used to record IP addresses obtained from the DHCP server, MAC addresses, the number of the port through which a client is connected to the DHCP-snooping-enabled device, and the number of the VLAN to which the port belongs to. These records are saved as entries in the DHCP-snooping table.

IP static binding table

The DHCP-snooping table only records information about clients that obtains IP address dynamically through DHCP. If a fixed IP address is configured for a client, the IP address and MAC address of the client cannot be recorded in the DHCP-snooping table. Consequently, this client cannot pass the IP filtering of the DHCP-snooping table, thus it cannot access external networks.

To solve this problem, the switch supports the configuration of static binding table entries, that is, the binding relationship between IP address, MAC address, and the port connecting to the client, so that packets of the client can be correctly forwarded.

IP filtering

The switch can filter IP packets in the following two modes:

- Filtering the source IP address in a packet. If the source IP address and the number of the port that receives the packet are consistent with entries in the DHCP-snooping table or static binding table, the switch regards the packet as a valid packet and forwards it; otherwise, the switch drops it directly.
- Filtering the source IP address and the source MAC address in a packet. If the source IP address and source MAC address in the packet, and the number of the port that receives the packet are consistent with entries in the DHCP-snooping table or static binding table, the switch regards the packet as a valid packet and forwards it; otherwise, the switch drops it directly.

DHCP Snooping Configuration

Configuring DHCP Snooping

Table 497 Configure the DHCP snooping function

Operation	Command	Description
Enter system view	**system-view**	-
Enable the DHCP snooping function	**dhcp-snooping**	Required By default, the DHCP snooping function is disabled
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Set the port connected to a DHCP server to a trusted port	**dhcp-snooping trust**	Required By default, all ports of a switch are untrusted ports

- *DHCP relay agent and DHCP snooping cannot be enabled at the same time. If you have enabled DHCP relay agent on the device, you will fail to enable DHCP snooping.*
- *The **dhcp-snooping trust** command and the **dhcp-snooping** command must be configured at the same time; otherwise DHCP packets may be dropped in actual networking.*

Configuring DHCP Snooping to Support Option 82

Enable DHCP snooping and specify trusted ports on the switch before configuring DHCP snooping to support Option 82.

Table 498 DHCP-snooping Option 82 support configuration tasks

Configuration task	Description	Related section
Enable DHCP-snooping Option 82 support	Required	"Enabling DHCP-snooping Option 82 support" on page 629
Configure a handling policy for DHCP packets with Option 82	Optional	"Configuring DHCP Snooping to Support Option 82" on page 628 "Configuring a handling policy for DHCP packets with Option 82" on page 629
Configure the storage format of Option 82	Optional	"Configuring DHCP Snooping to Support Option 82" on page 628 "Configuring the storage format of Option 82" on page 630

Table 498 DHCP-snooping Option 82 support configuration tasks

Configuration task	Description	Related section
Configure the circuit ID sub-option	Optional	"Configuring DHCP Snooping to Support Option 82" on page 628 "Configuring the circuit ID sub-option" on page 630
Configure the remote ID sub-option	Optional	"Configuring DHCP Snooping to Support Option 82" on page 628 "Configuring the remote ID sub-option" on page 630
Configure the padding format for Option 82	Optional	"Configuring DHCP Snooping to Support Option 82" on page 628 "Configuring the padding format for Option 82" on page 631

Enabling DHCP-snooping Option 82 support

Table 499 Enable DHCP-snooping Option 82 support

Operation	Command	Description
Enter system view	**system-view**	-
Enable DHCP-snooping Option 82 support	**dhcp-snooping information enable**	Required Disabled by default.

Configuring a handling policy for DHCP packets with Option 82

Table 500 Configure a handling policy for DHCP packets with Option 82

Operation	Command	Description
Enter system view	**system-view**	-
Configure a global handling policy for requests that contain Option 82	**dhcp-snooping information strategy** { **drop** | **keep** | **replace** }	Optional The default handling policy is **replace**.
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Configure a handling policy for requests that contain Option 82 received on the specified interface	**dhcp-snooping information strategy** { **drop** | **keep** | **replace** }	Optional The default policy is **replace**.



If a handling policy is configured on a port, this configuration overrides the globally configured handling policy for requests received on this port, while the globally configured handling policy applies on those ports where a handling policy is not natively configured.

Configuring the storage format of Option 82

The Switch 7750 supports the HEX or ASCII format for the Option 82 field.

Table 501 Configure a storage format for the Option 82 field

Operation	Command	Description
Enter system view	**system-view**	-
Configure a storage format for the Option 82 field	**dhcp-snooping information format** { **hex | ascii** }	Optional By default, the format is **hex**.

*The **dhcp-snooping information format** command applies only to the default content of the Option 82 field. If you have configured the circuit ID or remote ID sub-option, the format of the sub-option is ASCII, instead of the one specified with the **dhcp-snooping information format** command.*

Configuring the circuit ID sub-option

Table 502 Configure the circuit ID sub-option

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Configure the circuit ID sub-option in Option 82	**dhcp-snooping information** [**vlan** *vlan-id*] **circuit-id string** *string*	Optional By default, the circuit ID sub-option contains the VLAN ID and port index related to the port that receives DHCP request packets from DHCP clients

- *If you have configured a circuit ID with the **vlan** vlan-id argument specified, and the other one without the argument in Ethernet port view, the former circuit ID applies to the DHCP messages from the specified VLAN; while the latter one applies to DHCP messages from other VLANs.*
- *In a port aggregation group, you can use this command to configure the primary and member ports respectively. When Option 82 is added, however, the circuit ID sub-option is subject to the one configured on the primary port.*
- *The circuit ID sub-option configured on a port will neither be synchronized in the case of port aggregation.*

Configuring the remote ID sub-option

You can configure the remote ID sub-option in system view or Ethernet port view:

- In system view, the remote ID takes effect on all interfaces. You can configure Option 82 as the system name of the device or any customized character string in the ASCII format.
- In Ethernet port view, the remote ID takes effect only on the current interface. You can configure Option 82 as any customized character string in the ASCII format for different VLANs. That is to say, you can add different configuration rules for packets from different VLANs.

Table 503 Configure the remote ID sub-option in Option 82

Operation	Command	Description
Enter system view	**system-view**	-
Configure the remote ID sub-option in system view	**dhcp-snooping information remote-id** { **sysname | string** *string* }	Optional By default, the remote ID sub-option is the MAC address of the DHCP snooping device that received the DHCP client's request.
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Configure the remote ID sub-option in Ethernet port view	**dhcp-snooping information** [**vlan** *vlan-id*] **remote-id string** *string*	Optional By default, the remote ID sub-option is the MAC address of the DHCP snooping device that received the client's request.



- *If you configure a remote ID sub-option in both system view and on a port, the remote ID sub-option configured on the port applies when the port receives a packet, and the global remote ID applies to other interfaces that have no remote ID sub-option configured.*
- *If you have configured a remote ID with the **vlan** vlan-id argument specified, and the other one without the argument in Ethernet port view, the former remote ID applies to the DHCP messages from the specified VLAN, while the latter one applies to DHCP messages from other VLANs.*
- *In a port aggregation group, you can use this command to configure the primary and member ports respectively. When Option 82 is added, however, the remote ID is subject to the one configured on the primary port.*
- *The remote ID configured on a port will neither be synchronized in the case of port aggregation.*

Configuring the padding format for Option 82

Table 504 Configure the padding format for Option 82

Operation	Command	Description
Enter system view	**system-view**	-
Configure the padding format	**dhcp-snooping information packet-format** { **extended | standard** }	Optional By default, the padding format is in extended format.

Configuring IP Filtering

Table 505 Configure IP filtering

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Enable IP filtering	**ip check source ip-address** [**mac-address**]	Required By default, this function is disabled.

Table 505 Configure IP filtering

Operation	Command	Description
Create a static binding	**ip source static binding ip-address** *ip-address* [**mac-address** *mac-address*]	Optional By default, no static binding entry is created.

- *Enable DHCP snooping and specify trusted ports on the switch before configuring IP filtering.*
- *You are not recommended to configure IP filtering on the ports of an aggregation group.*

Displaying and Maintaining DHCP Snooping

After the above configuration, execute the **display** command in any view to display and verify the DHCP snooping configuration.

Execute the **reset** command in user view to clear the IP-MAC mappings recorded by the DHCP-Snooping-enabled switch.

Table 506 Display and maintain DHCP snooping configuration

Operation	Command	Description
Display the IP-MAC mappings recorded by the DHCP-Snooping-enabled switch	**display dhcp-snooping**	You can execute the **display** command in any view.
Display DHCP-Snooping status and trusted port information	**display dhcp-snooping trust**	
Display the total number of DHCP-Snooping binding table entries	**display dhcp-snooping count**	
Display the DHCP-Snooping binding table entries of the specified VLAN	**display dhcp-snooping vlan** { *vlan-list* | **all** }	
Display IP static binding table entries	**display ip source static binding** [**vlan** *vlan-id* | **interface** *interface-type interface-number*]	
Clear the IP-MAC mappings recorded by the DHCP-Snooping-enabled switch	**reset dhcp-snooping** [*ip-address*]	You can execute the **reset** command in user view.

DHCP Snooping Configuration Example

DHCP Snooping Trusted Port Configuration Example

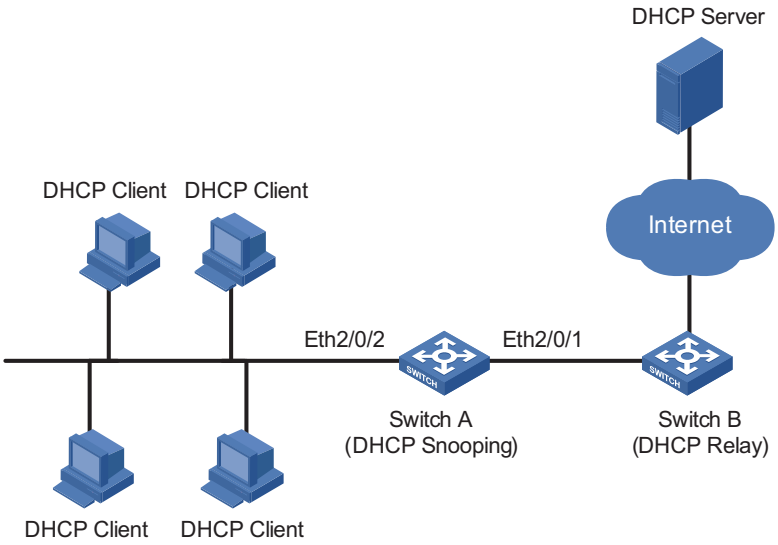
Network requirements

As shown in Figure 163, the Ethernet 2/0/1 port of Switch A is connected to Switch B (acting as a DHCP relay agent). A network segment containing some DHCP clients is connect to the Ethernet 2/0/2 port of Switch A.

- The DHCP snooping function is enabled on Switch A.
- The DHCP-Snooping-enabled device supports option 82 and option 82 is enabled on the switch.
- The Ethernet 2/0/1 port of Switch A is a trusted port.

Network diagram

Figure 163 DHCP-Snooping configuration



Configuration procedure

Perform the following configuration on the DHCP-Snooping-enabled Switch A.

Enter system view.

```
<SW7750> system-view
```

Enable the DHCP snooping function.

```
[SW7750] dhcp-snooping
```

Enable DHCP-Snooping option 82.

```
[SW7750] dhcp-Snooping information enable
```

Enter Ethernet 2/0/1 port view.

```
[SW7750] interface ethernet2/0/1
```

Specify the port as a trusted port.

```
[SW7750-Ethernet2/0/1] dhcp-snooping trust
```

DHCP-Snooping Option 82 Support Configuration Example

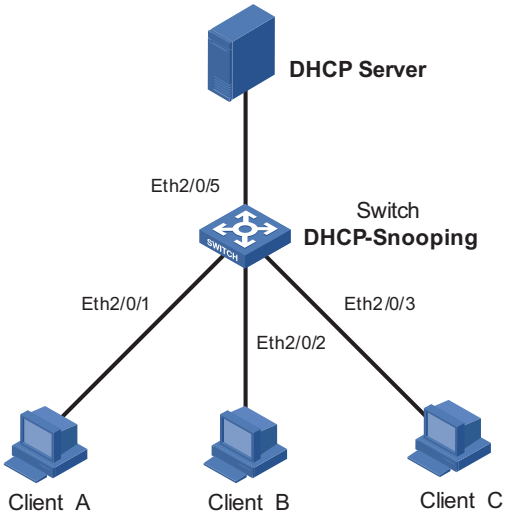
Network requirements

As shown in Figure 164, Ethernet 2/0/5 of the switch is connected to the DHCP server, and Ethernet 2/0/1, Ethernet 2/0/2, and Ethernet 2/0/3 are respectively connected to DHCP Client A, DHCP Client B, and DHCP Client C.

- Enable DHCP snooping on the switch.
- Specify Ethernet 2/0/5 on the switch as a trusted port for DHCP snooping.
- Enable DHCP-snooping Option 82 support on the switch and set the remote ID field in Option 82 to the system name of the switch. Set the circuit ID sub-option to **abcd** in DHCP packets from VLAN 1 on Ethernet 2/0/3.

Network diagram

Figure 164 Network diagram for DHCP-snooping Option 82 support configuration



Configuration procedure

Enable DHCP snooping on the switch.

```
<Switch> system-view
[Switch] dhcp-snooping
```

Specify Ethernet 2/0/5 as the trusted port.

```
[Switch] interface Ethernet2/0/5
[Switch-Ethernet2/0/5] dhcp-snooping trust
[Switch-Ethernet2/0/5] quit
```

Enable DHCP-snooping Option 82 support.

```
[Switch] dhcp-snooping information enable
```

Set the remote ID sub-option in Option 82 to the system name of the DHCP snooping device.

```
[Switch] dhcp-snooping information remote-id sysname
```

Set the circuit ID sub-option in DHCP packets from VLAN 1 to **abcd** on Ethernet 2/0/3.

```
[Switch] interface Ethernet2/0/3
[Switch-Ethernet2/0/3] dhcp-snooping information vlan 1 circuit-id s
tring abcd
```

IP Filtering Configuration Example

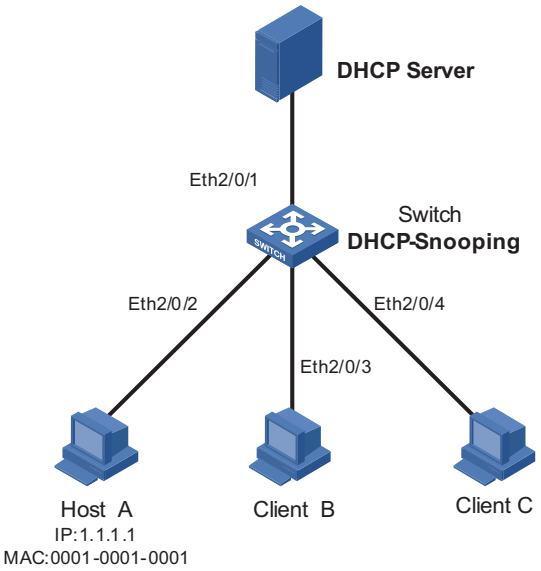
Network requirements

As shown in Figure 165, Ethernet 2/0/1 of the Switch 7750 is connected to the DHCP server and Ethernet 2/0/2 is connected to Host A. The IP address and MAC address of Host A are 1.1.1.1 and 0001-0001-0001 respectively. Ethernet 2/0/3 and Ethernet 2/0/4 are connected to DHCP Client B and Client C.

- Enable DHCP snooping on the switch, and specify Ethernet 2/0/1 as the DHCP snooping trusted port.
- Enable IP filtering on Ethernet 2/0/2, Ethernet 2/0/3, and Ethernet 2/0/4 to prevent attacks to the server from clients using fake source IP addresses.
- Create static binding entries on the switch, so that Host A using a fixed IP address can access external networks.

Network diagram

Figure 165 Network diagram for IP filtering configuration



Configuration procedure

Enable DHCP snooping on the switch.

```
<Switch> system-view
[Switch] dhcp-snooping
```

Specify Ethernet 2/0/1 as the trusted port.

```
[Switch] interface Ethernet2/0/1
[Switch-Ethernet2/0/1] dhcp-snooping trust
[Switch-Ethernet2/0/1] quit
```

Enable IP filtering on Ethernet 2/0/2, Ethernet 2/0/3, and Ethernet 2/0/4 to filter packets based on the source IP addresses/MAC addresses.

```
[Switch] interface Ethernet2/0/2
[Switch-Ethernet2/0/2] ip check source ip-address mac-address
[Switch-Ethernet2/0/2] quit
[Switch] interface Ethernet2/0/3
[Switch-Ethernet2/0/3] ip check source ip-address mac-address
[Switch-Ethernet2/0/3] quit
[Switch] interface Ethernet2/0/4
[Switch-Ethernet2/0/4] ip check source ip-address mac-address
[Switch-Ethernet2/0/4] quit
```

Create static binding entries on Ethernet 2/0/2 of the switch.

```
[Switch] interface Ethernet2/0/2
[Switch-Ethernet2/0/2] ip source static binding ip-address 1.1.1.1 m
ac-address 0001-0001-0001
```

60 ACL CONFIGURATION

Type A I/O Modules refer to the following: 3C16860, 3C16861, LS81FS24A, 3C16858, 3C16859, 3C16860, 3C16861, LS81FS24, 3C16858, and 3C16859.

ACL Overview

An access control list (ACL) is used primarily to identify traffic flows. In order to filter data packets, a series of match rules must be configured on the network device to identify the packets to be filtered. After the specific packets are identified, and based on the predefined policy, the network device can permit/prohibit the corresponding packets to pass.

ACLs classify packets based on a series of match conditions, which can be the source addresses, destination addresses and port numbers carried in the packets.

The packet match rules defined by ACLs can be referenced by other functions that need to differentiate traffic flows, such as the definition of traffic classification rules in QoS.

According to the application purpose, ACLs fall into the following four types:

- Basic ACL: rules are made based on the L3 source IP addresses only.
- Advanced ACL: rules are made based on the L3 and L4 information such as the source and destination IP addresses of the data packets, the type of protocol over IP, protocol-specific features, and so on.
- Layer 2 ACL: rules are made based on the Layer 2 information such as the source and destination MAC address information, VLAN priority, Layer 2 protocol, and so on.
- User-defined ACL: such rules specify a byte in the packet, by its offset from the packet header, as the starting point to perform logical AND operations, and compare the extracted string with the user-defined string to find the matching packets for processing.

Ways to Apply ACL on a Switch

ACLs activated directly on the hardware

In the switch, an ACL can be directly activated on the hardware for packet filtering and traffic classification in the data forwarding process. In this case, the match order of multiple rules in an ACL is determined by the hardware of the switch, and any user-defined match order, even if it is configured when the ACL is defined, will not work.

ACLs are directly activated on the switch hardware in the following situations: the switch references ACLs to implement the QoS functions, and the forwards data through ACLs.

ACL referenced by the upper-level modules

The switch also uses ACLs to filter packets processed by software and implements traffic classification. In this case, there are two types of match orders for the rules in an ACL: **config** (user-defined match order) and **auto** (the system performs automatic ordering, namely according "depth-first" order). In this scenario, you can specify the match order for multiple rules in an ACL. You cannot modify the match order for an ACL once you have specified it. You can specify a new the match order only after all the rules are deleted from the ACL.

ACLs can also be referenced by route policies or be used to control login users.

ACL Match Order

An ACL may contain a number of rules, which specify different packet ranges. This brings about the issue of match order when these rules are used to match packets.

An ACL supports the following two types of match orders:

- Configured order: ACL rules are matched according to the configured order.
- Automatic ordering: ACL rules are matched according to the "depth-first" order.

IP ACL depth-first order

With the depth-first rule adopted, the rules of an IP ACL (basic and advanced ACL) are matched in the following order:

1. Protocol number of ACL rules. Protocol number ranges from 1 to 255. The smaller the protocol range, the higher the priority.
2. Range of source IP address. The smaller the source IP address range (that is, the longer the mask), the higher the priority.
3. Range of destination IP address. The smaller the destination IP address range (that is, the longer the mask), the higher the priority.
4. Range of Layer 4 port number, that is, of TCP/UDP port number. The smaller the range, the higher the priority.

If rule A and rule B are the same in all the four ACEs (access control elements) above, and also in their numbers of other ACEs to be considered in deciding their priority order, weighting principles will be used in deciding their priority order.

The weighting principles work as follows:

- Each ACE is given a fixed weighting value. This weighting value and the value of the ACE itself will jointly decide the final matching order.
- The weighting values of ACEs rank in the following descending order: DSCP, ToS, ICMP, established, precedence, fragment.
- A fixed weighting value is deducted from the weighting value of each ACE of the rule. The smaller the weighting value left, the higher the priority.
- If the number and type of ACEs are the same for multiple rules, then the sum of ACE values of a rule determines its priority. The smaller the sum, the higher the priority.

Layer 2 ACL depth-first order

With the depth-first rule adopted, the rules of a Layer 2 ACL are matched in the order of the mask length of the source MAC address and destination MAC address. The longer of the mask is, the higher the match priority is. If two mask lengths are the same, the priority of the match rule configured earlier is higher. For example, the priority of the match rule with source MAC address mask FFFF-FFFF-0000 is higher then the priority of the match rule with source MAC address mask FFFF-0000-0000.

ACLs Based on Time Ranges

A time range-based ACL enables you to implement ACL control over packets by differentiating the time ranges.

A time range can be specified in each rule in an ACL. If the time range specified in a rule is not configured, the system will give a prompt message and allow such a rule to be successfully created. However, the rule does not take effect immediately. It takes effect only when the specified time range is configured and the system time is within the time range. If you remove the time range of an ACL rule, the ACL rule becomes invalid the next time the ACL rule timer refreshes.

Types of ACLs Supported by the Ethernet Switch

The following types of ACLs are supported by the Ethernet switch:

- Basic ACL
- Advanced ACL
- Layer 2 ACL
- User-defined ACL

Choosing ACL Mode for Traffic Flows

A switch can only choose one ACL mode for traffic flows, Layer 2 ACL mode or Layer 3 ACL mode. In Layer 2 ACL mode, only Layer 2 ACL can be activated or referenced by other applications, and Layer 3 ACL is similar.

Configuration Procedure

Table 507 Configure ACL mode for traffic flows

Operation	Command	Description
Enter system view	**system-view**	-
Configure ACL mode for traffic flows	**acl mode** { **ip-based** | **link-based** }	Required By default, a switch chooses **ip-based** ACL mode for traffic flows, that is, ACL classifies the traffic flows based on Layer 3 information.
Display the ACL mode for traffic flows	**display acl mode**	Optional The **display** command can be executed in any view



This configuration is only effective on Type A I/O Modules.

Configuration Example

Configure the ACL mode for traffic flows as **link-based**.

```
<SW7750> system-view
[SW7750] acl mode link-based
[SW7750] display acl mode
 The current acl mode: link-based.
```

Specifying the Matching Order of ACL Rules Sent to a Port

The **acl match-order** { **config** | **auto** } command is used to set the matching order of ACL rules when they are referenced by softwares. While the **acl order** command is used to set the matching order of ACL rules after they are applied to hardware). The Switch 7750 supports three matching orders of ACL rules applied to a port: **depth-first**, **first-config-first-match**, and **last-config-first match**. You can specify one of the three orders.

Configuration Procedure

Table 508 Set the matching order of ACL rules applied to a port

Operation	Command	Description
Enter system view	**system-view**	-
Set the matching order of the configured ACL rules sent to a port	**acl order** { **auto** | **first-config-first-match** | **last-config-first-match** }	Required By default, the configured ACL rules sent to a port match in the **depth-first** order, that is, the **auto** mode.
Display the matching order of the ACL rules applied to a port	**display acl order**	Optional The **display** command can be executed in any view

Configuration Example

Specify the matching order of ACL rules sent to hardware as **first-config-first-match**.

```
<SW7750> system-view
[SW7750] acl order first-config-first-match
[SW7750] display acl order
the current order is first-config-first-match
```

Configuring Time Ranges

The time range configuration tasks include configuring periodic time sections and configuring absolute time sections. A periodic time section appears as a period of time in a day of the week, while an absolute time section appears in the form of "the start time to the end time".

Configuration Procedure

Table 509 Configure a time range

Operation	Command	Description
Enter system view	**system-view**	-
Create a time range	**time-range** *time-name* { *start-time* **to** *end-time days-of-the-week* [**from** *start-time start-date*] [**to** *end-time end-date*] | **from** *start-time start-date* [**to** *end-time end-date*] | **to** *end-time end-date* }	Required

Table 509 Configure a time range

Operation	Command	Description
Display a time range or all the time ranges	**display time-range** { **all** | *time-name* }	Optional This command can be executed in any view.

Note that:

- If only a periodic time section is defined in a time range, the time range is active only within the defined periodic time section.
- If only an absolute time section is defined in a time, the time range is active only within the defined absolute time section.
- If both a periodic time section and an absolute time section are defined in a time range, the time range is active only when the periodic time range and the absolute time range are both matched. Assume that a time range defines an absolute time section from 00:00 January 1, 2004 to 23:59 December 31, 2004, and a periodic time section from 12:00 to 14:00 every Wednesday. This time range is active only from 12:00 to 14:00 every Wednesday in 2004.
- If the start time is not specified, the time range starts from the smallest time that the system can get and ends on the end date.
- If the end date is note specified, the time range is from the date of configuration till the largest date available in the system.

Configuration Example

Define a periodic time section "test" that will be active from 8:00 to 18:00 Monday through Friday.

```
<SW7750> system-view
[SW7750] time-range test 8:00 to 18:00 working-day
[SW7750] display time-range test
Current time is 11:14:19 4-27-2006 Thursday

Time-range : test ( Active )
 08:00 to 18:00 working-day
```

Defining Basic ACLs

A basic ACL defines rules only based on the L3 source IP addresses to analyze and process data packets.

The value range for basic ACL numbers is 2,000 to 2,999.

Configuration Preparation

Before configuring an ACL rule containing time range arguments, you need to define the corresponding time ranges. For the configuration of time ranges, refer to "Configuring Time Ranges" on page 640

The source IP address in the rule has been defined.

Configuration Procedure

Table 510 Define a basic ACL rule

Operation	Command	Description
Enter system view	**system-view**	-

Table 510 Define a basic ACL rule

Operation	Command	Description
Create or enter basic ACL view	**acl** { **number** *acl-number* | **name** *acl-name* [**advanced** | **basic** | **link** | **user**] } [**match-order** { **config** | **auto** }]	Required By the default, the match order is **config**.
Define an rule	**rule** [*rule-id*] { **permit** | **deny** } [**source** { *source-addr wildcard* | **any** } | **fragment** | **time-range** *time-name*]*	Required
Display ACL information	**display acl config** { **all** | *acl-number* | *acl-name* }	Optional This command can be executed in any view.

In the case that you specify the rule ID when defining a rule:

- If the rule corresponding to the specified rule ID already exists, you will edit the rule, and the modified part in the rule will replace the original content, while other parts remain unchanged.
- If the rule corresponding to the specified rule ID does not exists, you will create and define a new rule.
- The content of a newly created rule must not be identical with the content of any existing rule; otherwise the rule creation will fail, and the system will prompt that the rule already exists.

If you do not specify a rule ID, you will create and define a new rule, and the system will assign an ID for the rule automatically.

Configuration Example

Configure ACL 2000 to deny packets whose source IP address is 1.1.1.1.

```
<SW7750> system-view
[SW7750] acl number 2000
[SW7750-acl-basic-2000] rule deny source 1.1.1.1 0
[SW7750-acl-basic-2000] display acl config 2000
Basic ACL  2000, 1 rule,
rule 0 deny source 1.1.1.1 0 (0 times matched)
```

Defining Advanced ACLs

Advanced ACLs define classification rules according to the source and destination IP addresses of packets, the type of protocol over IP, and protocol-specific features such as TCP/UDP source and destination ports, TCP flag bit, ICMP protocol type, and so on.

The value range for advanced ACL numbers is 3,000 to 3,999 (ACL 3998 and 3999 are reserved for cluster management, and you cannot configure them).

Advanced ACLs support analysis and processing of three packet priority levels: type of service (ToS) priority, IP priority and differentiated services codepoint Priority (DSCP).

Using advanced ACLs, you can define classification rules that are more accurate, more abundant, and more flexible than those defined with basic ACLs.

Configuration Preparation

Before configuring an ACL rule containing time range arguments, you need to configure define the corresponding time ranges. For the configuration of time ranges, refer to "Configuring Time Ranges" on page 640.

The values of source and destination IP addresses, the type of the protocols carried by IP, and protocol-specific features in the rule have been defined.

Configuration Procedure

Table 511 Define an advanced ACL rule

Operation	Command	Description
Enter system view	**system-view**	-
Create or enter advanced ACL view	**acl** { **number** *acl-number* | **name** *acl-name* [**advanced** | **basic** | **link** | **user**] } [**match-order** { **config** | **auto** }]	Required By the default, the match order is **config**.
Define an rule	**rule** [*rule-id*] { **permit** | **deny** } *rule-string*	Required
Display ACL information	**display acl config** { **all** | *acl-number* | *acl-name* }	Optional This command can be executed in any view.

rule-string: rule information, which can be combination of the parameters described in Table 512. You must configure the *protocol* argument in the rule information before you can configure other arguments.

Table 512 Rule information

Parameter	Type	Function	Description
protocol	Protocol type	Type of protocol over IP	When expressed in numerals, the value range is 1 to 255. When expressed with a name, the value can be GRE, ICMP, IGMP, IP, IPinIP, OSPF, TCP, and UDP.
source { *sour-addr sour-wildcard* | **any** }	Source address information	Specifies the source address information in the rule	*sour-addr sour-wildcard* is used to specify the source address of the packet, expressed in dotted decimal notation. **any** represents all source addresses.
destination { *dest-addr dest-wildcard* | **any** }	Destination address information	Specifies the destination address information in the rule	*dest-addr dest-wildcard* is used to specify the destination address of the packet, expressed in dotted decimal notation. **any** represents all destination address.
precedence *precedence*	Packet precedence	Packet priority	Value range: 0 to 7

Table 512 Rule information

Parameter	Type	Function	Description
tos *tos*	Packet precedence	ToS priority	Value range: 0 to 15
dscp *dscp*	Packet precedence	DSCP priority	Value range: 0 to 63
fragment	Fragment information	Specifies that the ACL rule is effective for non-initial fragment packets	-
time-range *time-name*	Time range information	Specifies the time range in which the ACL rule is active	-

sour-wildcard and dest-wildcard represent the wildcard masks of the destination subnet masks, provided in dotted decimal. For example, if you want to specify the subnet mask as 255.255.0.0, you need to input 0.0.255.255. The wildcard mask can be 0, representing the host address.

To define DSCP priority, you can directly input a value ranging from 0 to 63, or input a keyword listed in Table 513.

Table 513 Description of DSCP values

Keyword	DSCP value in decimal	DSCP value in binary
ef	46	101110
af11	10	001010
af12	12	001100
af13	14	001110
af21	18	010010
af22	20	010100
af23	22	010110
af31	26	011010
af32	28	011100
af33	30	011110
af41	34	100010
af42	36	100100
af43	38	100110
cs1	8	001000
cs2	16	010000
cs3	24	011000
cs4	32	100000
cs5	40	101000
cs6	48	110000
cs7	56	111000
be (default)	0	000000

To define the IP precedence, you can directly input a value ranging from 0 to 7, or input a keyword listed in the following table.

Table 514 Description of IP precedence value

Keyword	IP Precedence value in decimal	IP Precedence value in binary
routine	0	000
priority	1	001
immediate	2	010
flash	3	011
flash-override	4	100
critical	5	101
internet	6	110
network	7	111

To define the ToS value, you can directly input a value ranging from 0 to 15, or input a keyword listed in the following table.

Table 515 Description of ToS value

Keyword	ToS value in decimal	ToS value in binary
normal	0	0000
min-monetary-cost	1	0001
max-reliability	2	0010
max-throughput	4	0100
min-delay	8	1000

If the protocol type is TCP or UDP, you can also define the following information:

Table 516 TCP/UDP-specific rule information

Parameter	Type	Function	Description
source-port *operator port1* [*port2*]	Source port(s)	Defines the source port information of UDP/TCP packets	The value of *operator* can be lt (less than), gt (greater than), eq (equal to), neq (not equal to) or range (within the range of) Only the "range" operator requires two port numbers as the operands, and other operators require only one port number as the operand *port1* and *port2*: TCP/UDP port number(s), expressed with name(s) or numerals; when expressed with numerals, the value range is 0 to 65,535
destination-port *operator port1* [*port2*]	Destination port(s)	Defines the destination port information of UDP/TCP packets	
established	TCP connection established" flag	Indicates that the ACL rule is only valid for the first SYN packet (when the TCP connection began)	TCP-specific argument

Only Type A I/O Modules support the "range" operation on the TCP/UDP port.

If the protocol type is ICMP, you can also define the following information:

Table 517 ICMP-specific rule information

Parameter	Type	Function	Description
icmp-type *icmp-type icmp-code*	Type and message code information of ICMP packets	Specifies the type and message code information of ICMP packets in the ACL rule	*icmp-type*: ICMP message type, ranging 0 to 255 *icmp-code*: ICMP message code, ranging 0 to 255

If the protocol type is ICMP, you can also directly input the ICMP message name after the **icmp-type** argument. The following table describes some common ICMP messages.

Table 518 ICMP messages

Name	ICMP TYPE	ICMP CODE
echo	Type=8	Code=0
echo-reply	Type=0	Code=0
fragmentneed-DFset	Type=3	Code=4
host-redirect	Type=5	Code=1
host-tos-redirect	Type=5	Code=3
host-unreachable	Type=3	Code=1
information-reply	Type=16	Code=0
information-request	Type=15	Code=0
net-redirect	Type=5	Code=0
net-tos-redirect	Type=5	Code=2
net-unreachable	Type=3	Code=0
parameter-problem	Type=12	Code=0
port-unreachable	Type=3	Code=3
protocol-unreachable	Type=3	Code=2
reassembly-timeout	Type=11	Code=1
source-quench	Type=4	Code=0
source-route-failed	Type=3	Code=5
timestamp-reply	Type=14	Code=0
timestamp-request	Type=13	Code=0
ttl-exceeded	Type=11	Code=0

In the case that you specify the rule ID when defining a rule:

- If the rule corresponding to the specified rule ID already exists, you will edit the rule, and the modified part in the rule will replace the original content, while other parts remain unchanged.
- If the rule corresponding to the specified rule ID does not exists, you will create and define a new rule.

- The content of a newly created rule must not be identical with the content of any existing rule; otherwise the rule creation will fail, and the system will prompt that the rule already exists.

If you do not specify a rule ID, you will create and define a new rule, and the system will assign an ID for the rule automatically.

Configuration Example

Configure ACL 3000 to permit TCP packets to pass. The port number of the packets is 80, the source network segment of packets is 129.9.0.0, and the destination network segment is 202.38.160.0

```
<SW7750> system-view
[SW7750] acl number 3000
[SW7750-acl-adv-3000] rule permit tcp source 129.9.0.0 0.0.255.255 d
estination 202.38.160.0 0.0.0.255 destination-port eq 80
[SW7750-acl-adv-3000] display acl config 3000
Advanced ACL  3000, 1 rule,
rule 0 permit tcp source 129.9.0.0 0.0.255.255 destination 202.38.16
0.0 0.0.0.255 destination-port eq www (0 times matched)
```

Defining Layer 2 ACLs

Layer 2 ACLs define rules based on the Layer 2 information such as the source and destination MAC address information, VLAN priority and Layer 2 protocol to process packets.

The value range for Layer 2 ACL numbers is 4,000 to 4,999.

Configuration Preparation

Before configuring an ACL rule containing time range arguments, you need to configure define the corresponding time ranges. For the configuration of time ranges, refer to "Configuring Time Ranges" on page 640.

The source and destination MAC addresses, VLAN priority and Layer 2 protocol in the rule have been defined.

Configuration Tasks

Table 519 Create a Layer 2 ACL rule

Operation	Command	Description
Enter system view	**system-view**	-
Create or enter layer 2 ACL view	**acl** { **number** *acl-number* | **name** *acl-name* [**advanced** | **basic** | **link** | **user**] } [**match-order** { **config** | **auto** }]	Required By default, the match order is **config**.
Define an ACL rule	**rule** [*rule-id*] { **permit** | **deny** } [*rule-string*]	Required If you do not specify the *rule-string* parameter, the switch will choose **ingress any egress** any by default.
Display ACL information	**display acl config** { **all** | *acl-number* | *acl-name* }	Optional This command can be executed in any view.

rule-string: rule information, which can be combination of the parameters described in Table 520.

Table 520 Rule information

Parameter	Type	Function	Description
protocol-type	Protocol type	Defines the protocol type over Ethernet frames	*protocol-type*: the value can be ip, arp, rarp, ipx, nbx, pppoe-control, or pppoe-data.
format-type	Link layer encapsulation type	Defines the link layer encapsulation type in the rule	*format-type*: the value can be 802.3/802.2, 802.3, ether_ii, or snap.
ingress { { *source-vlan-id* | *source-mac-addr* [*source-mac-mask*] } * | **any** }	Source MAC address information	Specifies the source MAC address range in the ACL rule	*source-mac-addr*: source MAC address, in the format of H-H-H *source-mac-mask*: source MAC address mask, in the format of H-H-H, defaults to ffff-ffff-ffff. *source-vlan-id*: source VLAN ID, in the range of 1 to 4,094 **any** represents all packets received from all ports.
egress { *dest-mac-addr* [*dest-mac-mask*] | **any** }	Destination MAC address information	Specifies the destination MAC address range in the ACL rule	*dest-mac-addr*: destination MAC address, in the format of H-H-H *dest-mac-mask*: destination MAC address mask, in the format of H-H-H, defaults to ffff-ffff-ffff. **any** represents all packets forwarded by all ports.
cos *cos*	Priority	Defines the 802.1p priority of the ACL rule	*cos*: ranges from 0 to 7
time-range *time-name*	Time range information	Specifies the time range in which the rule is active	*time-name*: specifies the name of the time range in which the ACL rule is active; a string of 1 to 32 characters

To define the CoS, you can directly input a value ranging from 0 to 7, or input a keyword listed in the following table.

Table 521 Description of CoS value

Keyword	CoS value in decimal	CoS value in binary
best-effort	0	000
background	1	001
spare	2	010
excellent-effort	3	011
controlled-load	4	100

Table 521 Description of CoS value

Keyword	CoS value in decimal	CoS value in binary
video	5	101
voice	6	110
network-management	7	111

In the case that you specify the rule ID when defining a rule:

- If the rule corresponding to the specified rule ID already exists, you will edit the rule, and the modified part in the rule will replace the original content, while other parts remain unchanged.
- If the rule corresponding to the specified rule ID does not exists, you will create and define a new rule.
- The content of a newly created rule must not be identical with the content of any existing rule; otherwise the rule creation will fail, and the system will prompt that the rule already exists.

If you do not specify a rule ID, you will create and define a new rule, and the system will assign an ID for the rule automatically.

Configuration Example

Configure ACL 4000 to deny packets whose 802.1p priority is 3, source MAC address is 000d-88f5-97ed, and destination MAC address is 0011-4301-991e.

```
<SW7750> system-view
[SW7750] acl number 4000
[SW7750-acl-link-4000] rule deny cos 3 source 000d-88f5-97ed ffff-ff
ff-ffff dest 0011-4301-991e ffff-ffff-ffff
[SW7750-acl-link-4000] display acl config 4000
Link ACL  4000, 1 rule,
rule 0 deny cos excellent-effort source 000d-88f5-97ed ffff-ffff-fff
f dest 0011-4301-991e ffff-ffff-ffff (0 times matched)
```

Defining User-Defined ACLs

Using a byte, which is specified through its offset from the packet header, in the packet as the starting point, user-defined ACLs perform logical AND operations on packets and compare the extracted string with the user-defined string to find the matching packets for processing.

User-defined ACL numbers range from 5,000 to 5,999.

Configuration Preparation

To configure a time range-based ACL rule, you need first to define the corresponding time range, as described in "Configuring Time Ranges" on page 640.

Configuration Procedure

Table 522 Define a user-defined ACL rule

Operation	Command	Description
Enter system view	**system-view**	-

Table 522 Define a user-defined ACL rule

Operation	Command	Description
Create or enter user-defined ACL view	**acl** { **number** *acl-number* | **name** *acl-name* [**advanced** | **basic** | **link** | **user**] } [**match-order** { **config** | **auto** }]	Required By default, the match order is **config**.
Define an ACL rule	**rule** [*rule-id*] { **permit** | **deny** } { *rule-string rule-mask offset* } &<1-8> [**time-range** *time-name*]	Required
Display ACL information	**display acl** { **all** | *acl-number* }	Optional This command can be executed in any view.

When you specify the rule ID by using the **rule** command, note that:

- You can specify an existing rule ID to modify the corresponding rule. ACEs that are not modified remain unchanged.
- You can create a rule by specifying an ID that identifies no rule.
- You will fail to create a rule if the newly created rule is the same as an existing one.

If you do not specify the rule ID when creating an ACL rule, the rule ID of the newly created rule is assigned by the system.



Only I/O Modules other than Type A support the user-defined ACL.

Configuration Example

Configure ACL 5001 to deny all TCP packets.

```
<SW7750> system-view
[SW7750] time-range t1 18:00 to 23:00 sat
[SW7750] acl number 5001
[SW7750-acl-user-5001] rule 25 deny 06 ff 27 time-range t1
[SW7750-acl-user-5001] display acl config 5001
User ACL  5001, 1 rule
rule 25 deny 06 ff 27 time-range t1 (0 times matched) (Inactive)
```

Applying ACLs on Ports

By applying ACLs on ports, you can filter certain packets.

Configuration Preparation

You need to define an ACL before applying it on a port. For operations to define ACLs, refer to "Defining Basic ACLs" on page 641, "Defining Advanced ACLs" on page 642, "Defining Layer 2 ACLs" on page 647, and "Defining User-Defined ACLs" on page 649.

Configuration Procedure

Table 523 Apply an ACL on a port

Operation	Command	Description
Enter system view	**system-view**	-

Table 523 Apply an ACL on a port

Operation	Command	Description
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Enter QoS view	**qos**	-
Apply an ACL on the port	**packet-filter** { **inbound** | **outbound** } *acl-rule* [**system-index** *system-index*] [**not-care-for-interface**]	Required This command is supported by Type A I/O Modules.
	packet-filter inbound *acl-rule* [**system-index** *system-index*]	Required This command is supported by I/O Modules other than Type A.
Display the ACL information sent to a port	**display acl running-packet-filter** { **all** | **interface** *interface-type interface-number* }	Optional This command can be executed in any view.

acl-rule: Applied ACL, which can be a combination of different types of ACL rules. Table 524 and Table 526 describe the ACL combinations on Type A I/O Modules and the corresponding parameter description. Table 525 and Table 526 describe the ACL combinations on I/O Modules other than Type A and the corresponding parameter description.

Table 524 Combined application of ACLs on Type A I/O Modules

Combination mode	Form of acl-rule
Apply all rules in an IP type ACL separately	**ip-group** { *acl-number* | *acl-name* }
Apply one rule in an IP type ACL separately	**ip-group** { *acl-number* | *acl-name* } **rule** *rule-id*
Apply all rules in a link type ACL separately	**link-group** { *acl-number* | *acl-name* }
Apply one rule in a link type separately	**link-group** { *acl-number* | *acl-name* } **rule** *rule-id*

Table 525 Combined application of ACLs on I/O Modules other than Type A.

Combination mode	Form of acl-rule
Apply all rules in an IP type ACL separately	**ip-group** { *acl-number* | *acl-name* }
Apply one rule in an IP type ACL separately	**ip-group** { *acl-number* | *acl-name* } **rule** *rule-id*
Apply all rules in a link type ACL separately	**link-group** { *acl-number* | *acl-name* }
Apply one rule in a link type separately	**link-group** { *acl-number* | *acl-name* } **rule** *rule-id*
Apply all rules in a user-defined ACL separately	**user-group** { *acl-number* | *acl-name* }
Apply one rule in a user-defined ACL separately	**user-group** { *acl-number* | *acl-name* } **rule** *rule-id*
Apply one rule in an IP type ACL and one rule in a Link type ACL simultaneously	**ip-group** { *acl-number* | *acl-name* } **rule** *rule-id* **link-group** { *acl-number* | *acl-name* } **rule** *rule-id*

Table 526 Parameters description of ACL combinations

Parameter	Description
ip-group { *acl-number* | *acl-name* }	Basic and advanced ACL. *acl-number*: ACL number, ranging from 2,000 to 3,999. *acl-name*: ACL name, up to 32 characters long, beginning with an English letter (a to z or A to Z) without space and quotation mark, case insensitive.
link-group { *acl-number* | *acl-name* }	Layer 2 ACL *acl-number*: ACL number, ranging from 4,000 to 4,999. *acl-name*: ACL name, up to 32 characters long, beginning with an English letter (a to z or A to Z) without space and quotation mark, case insensitive.
user-group { *acl-number* | *acl-name* }	User-defined ACL *acl-number*: ACL number, ranging from 5,000 to 5,999. *acl-name*: ACL name, up to 32 characters long, beginning with an English letter (a to z or A to Z) without space and quotation mark, case insensitive.
rule-id	Number of the ACL rule, ranging from 0 to 127. If this argument is not specified, all rules in the specified ACL will be applied.

Configuration Example

Apply ACL 2100 in the inbound direction on Ethernet 2/0/1 to filter packets.

```
<SW7750> system-view
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] qos
[SW7750-qoss-Ethernet2/0/1] packet-filter inbound ip-group 2100
```

Displaying ACL Configuration

After the above configuration, you can execute the **display** commands in any view to view the ACL running information, so as to verify the configuration result.

Table 527 Display ACL configuration

Operation	Command	Description
Display a time range or time ranges	**display time-range** { **all** | *time-name* }	These commands can be executed in any view.
Display the configured ACL rule(s)	**display acl config** { **all** | *acl-number* }	
Display the statistics information about the configured ACL rules	**display acl config statistics**	
Display the remain ACL resource of a specified slot	**display acl remaining entry slot** *slot-number*	
Display the ACL mode of traffic flows	**display acl mode**	
Display the ACL rules applied to a port	**display acl running-packet-filter** { **all** | **interface** *interface-type interface-number* }	
Display the matching order of the applied ACL rules	**display acl order**	

ACL Configuration Example

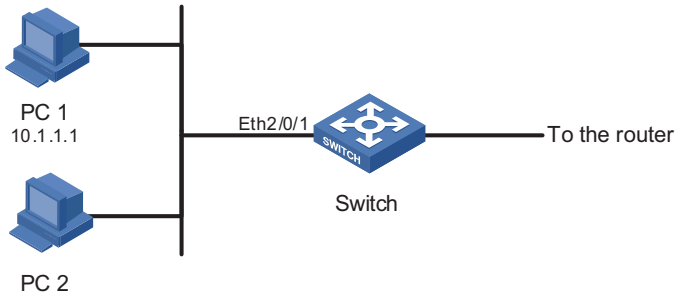
Basic ACL Configuration Example

Network requirements

Through basic ACL configuration, packets from the host with the source IP address of 10.1.1.1 (the host is connected to the switch through Ethernet 2/0/1 port) are to be filtered within the time range from 8:00 to 18:00 everyday.

Network diagram

Figure 166 Network diagram for basic ACL configuration



Configuration procedure

Only the commands related to the ACL configuration are listed below.

1 Define the time range

Define the time range from 8:00 to 18:00.

```
<SW7750> system-view
[SW7750] time-range test 8:00 to 18:00 daily
```

2 Define an ACL for packets with the source IP address of 10.1.1.1.

Enter ACL 2000.

```
[SW7750] acl number 2000
```

Define an access rule to deny packets with their source IP addresses being 10.1.1.1.

```
[SW7750-acl-basic-2000] rule 1 deny source 10.1.1.1 0 time-range test
[SW7750-acl-basic-2000] quit
```

3 Apply the ACL on the port

Apply ACL 2000 on the port.

```
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] qos
[SW7750-qosb-Ethernet2/0/1] packet-filter inbound ip-group 2000
```

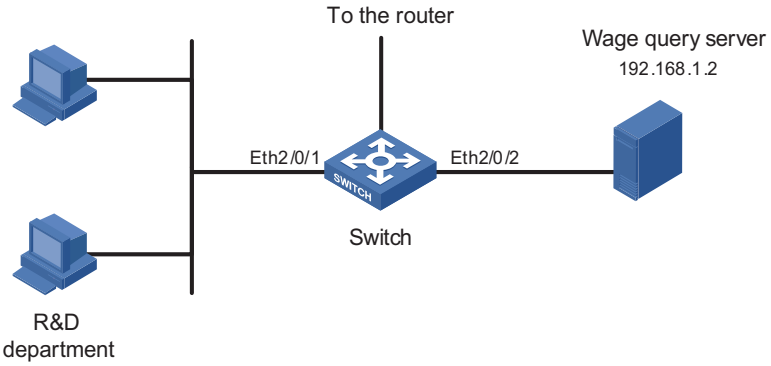
Advanced ACL Configuration Example

Network requirements

Different departments of an enterprise are interconnected on the intranet through the ports of a switch. The IP address of the wage query server is 192.168.1.2. Devices of the R&D department are connected to the Ethernet 2/0/1 port of the switch. Apply an ACL to deny requests sourced from the R&D department and destined for the wage server during the working hours (8:00 to 18:00).

Network diagram

Figure 167 Network diagram for advanced ACL configuration



Configuration procedure

Only the commands related to the ACL configuration are listed below.

1 Define the time range

Define a time range that contain a periodic time section from 8:00 to 18:00.

```
<SW7750> system-view
[SW7750] time-range test 8:00 to 18:00 working-day
```

2 Define an ACL for filtering requests destined for the wage server.

Create ACL 3000.

```
[SW7750] acl number 3000
```

Define an ACL rule for requests destined for the wage server.

```
[SW7750-acl-adv-3000] rule 1 deny ip destination 192.168.1.2 0 time-range test
[SW7750-acl-adv-3000] quit
```

3 Apply the ACL on a port.

Apply ACL 3000 on the Ethernet 2/0/1 port.

```
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] qos
[SW7750-qosb-Ethernet2/0/1] packet-filter inbound ip-group 3000
```

Layer 2 ACL Configuration Example

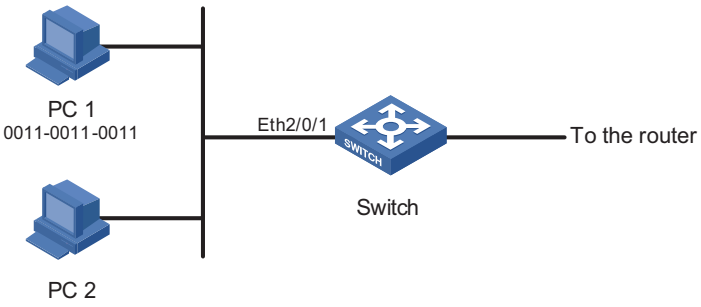
Network requirements

Through Layer 2 ACL configuration, packets with the source MAC address of 0011-0011-0011 and destination MAC address of 0011-0011-0012 are to be

filtered within the time range from 8:00 to 18:00 everyday. Apply this ACL on Ethernet 2/0/1 port.

Network diagram

Figure 168 Network diagram for Layer 2 ACL configuration



Configuration procedure

Only the commands related to the ACL configuration are listed below.

1 Define the time range

Define the time range ranging from 8:00 to 18:00.

```
<SW7750> system-view
[SW7750] time-range test 8:00 to 18:00 daily
```

2 Define an ACL rule for packets with the source MAC address of 0011-0011-0011 and destination MAC address of 0011-0011-0012.

Create ACL 4000.

```
[SW7750] acl number 4000
```

Define an ACL rule to deny packets with the source MAC address of 0011-0011-0011 and destination MAC address of 0011-0011-0012, specifying the time range named test for the ACL rule.

```
[SW7750-acl-link-4000] rule 1 deny ingress 0011-0011-0011 ffff-ffff-
ffff egress 0011-0011-0012 ffff-ffff-ffff time-range test
[SW7750-acl-link-4000] quit
```

3 Apply the ACL on a port.

Apply ACL 4000 on the port Ethernet 2/0/1.

```
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] qos
[SW7750-qosb-Ethernet2/0/1] packet-filter inbound link-group 4000
```

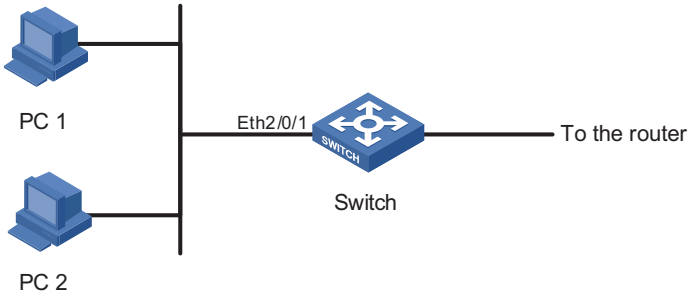
User-Defined ACL Configuration Example

Network requirements

Create a user-defined ACL to deny all TCP packets within the time range from 8:00 to 18:00 everyday. Apply the user-defined ACL on Ethernet 2/0/1 port.

Network diagram

Figure 169 Network diagram for user-defined ACL configuration



Configuration procedure

Only the commands related to the ACL configuration are listed below.

1 Define the time range.

Define the time range ranging from 8:00 to 18:00.

```
<SW7750> system-view
[SW7750] time-range aaa 8:00 to 18:00 daily
```

2 Create an ACL rule to filter TCP packets.

Create ACL 5000.

```
[SW7750] acl number 5000
```

Define a rule for TCP packets.

```
[SW7750-acl-user-5000] rule 1 deny 06 ff 27 time-range aaa
```

3 Apply the ACL on a port.

Apply ACL 5000 on the port Ethernet 2/0/1.

```
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] qos
[SW7750-qosb-Ethernet2/0/1] packet-filter inbound user-group 5000
```

61 QoS Configuration

- *Type-A I/O Modules include 3C16860, 3C16861, LS81FS24A, 3C16858, 3C16859, 3C16860, 3C16861, LS81FS24, 3C16858, and 3C16859.*
- *On type-A I/O Modules, the prompt for QoS view is **qoss**; on non-type-A I/O Modules, the prompt for QoS view is **qosb**.*

Overview

Quality of Service (QoS) is a concept generally existing in occasions with service supply and demand. It evaluates the ability to meet the need of the customers in service. Generally, the evaluation is not to grade precisely. Its purpose is to analyze the conditions when the service is the best and the conditions when the service still needs improvement and then to make improvements in the specified aspects.

In internet, QoS evaluates the ability of the network to deliver packets. The evaluation on QoS can be based on different aspects because the network provides various services. Generally speaking, QoS is the evaluation on the service ability to support the core requirements such as delay, delay variation and packet loss ratio in the packet delivery.

Traffic

Traffic means service traffic, that is, all the packets passing the switch.

Traffic Classification

Traffic classification means to identify packets conforming to certain characters according to certain rules.

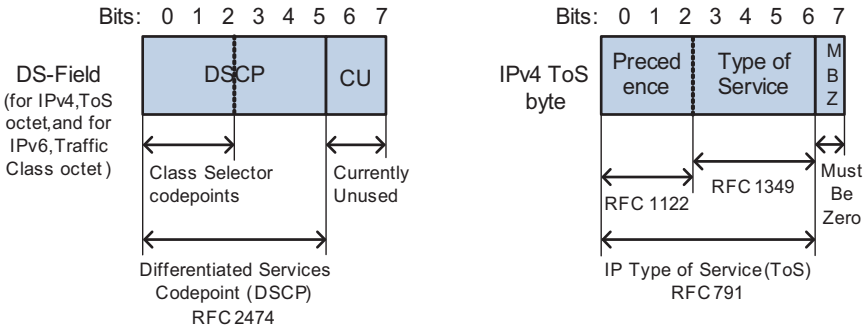
A classification rule is a filter rule configured to meet your management requirements. It can be very simple. For example, you can use a classification rule to identify traffic with different priorities according to the ToS field in the IP packet header. It can be very complicated too. For example, you can use a classification rule to identify the packets according to the combination of link layer (Layer 2), network layer (Layer 3) and transport layer (Layer 4) information including MAC addresses, IP protocols, source addresses, destination addresses, the port numbers of applications and so on.

Classification is generally based on the information in the packet header and rarely based on the packet content.

Precedence

1 IP precedence, ToS precedence and differentiated services code point (DSCP) precedence

Figure 170 DS fields and TOS bytes



The TOS field in an IP header contains 8 bits:

- The first three bits indicate IP precedence in the range of 0 to 7.
- Bit 3 to bit 6 indicate ToS precedence in the range of 0 to 15.
- RFC2474 re-defines the ToS field in the IP packet header, which is called the DS field. The first six (bit 0 to bit 5) bits of the DS field indicate DSCP precedence in the range of 0 to 63. The first three bits in DSCP precedence are class selector codepoints, bit 4 and bit 5 indicate drop precedence, and bit 6 is zero indicating that the device sets the service class with the DS model.
- The last two bits (bit 6 and bit 7) are reserved bits.

The precedence values of the IP packet indicate 8 different service classes.

Table 528 Description on IP Precedence

IP Precedence (decimal)	IP Precedence (binary)	Description
0	000	routine
1	001	priority
2	010	immediate
3	011	flash
4	100	flash-override
5	101	critical
6	110	internet
7	111	network

The Diff-Serv network defines four traffic classes:

- Expedited Forwarding (EF) class: In this class, packets can be forwarded regardless of link share of other traffic. The class is suitable for preferential services with low delay, low packet loss ratio, low variation and assured bandwidth (such as virtual leased line);
- Assured forwarding (AF) class: This class is further divided into four subclasses (AF1/2/3/4) and a subclass is further divided into three drop priorities, so the AF

service level can be segmented. The QoS rank of the AF class is lower than that of the EF class;

- Class selector (CS) class: This class comes from the IP TOS field and includes 8 classes;
- Best Effort (BE) class: This class is a special class without any assurance in the CS class. The AF class can be degraded to the BE class if it exceeds the limit. Current IP network traffic belongs to this class by default.

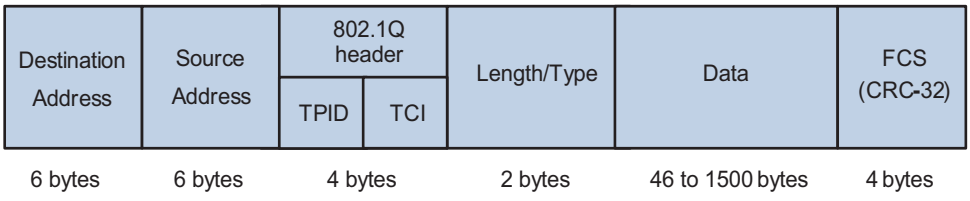
Table 529 Description on DSCP values

DSCP	DSCP value (decimal)	DSCP value (binary)
ef	46	101110
af11	10	001010
af12	12	001100
af13	14	001110
af21	18	010010
af22	20	010100
af23	22	010110
af31	26	011010
af32	28	011100
af33	30	011110
af41	34	100010
af42	36	100100
af43	38	100110
cs1	8	001000
cs2	16	010000
cs3	24	011000
cs4	32	100000
cs5	40	101000
cs6	48	110000
cs7	56	111000
default (be)	0	000000

2 802.1p priority

802.1p priority lies in Layer 2 packet headers and is applicable to occasions where the Layer 3 packet header does not need analysis but QoS must be assured in Layer 2.

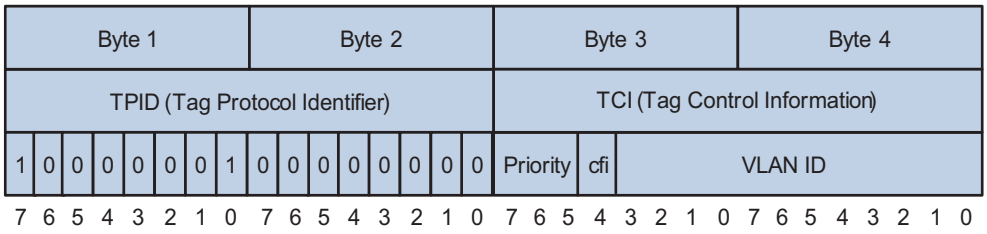
Figure 171 An Ethernet frame with a 802.1Q tag header



As shown in the figure above, each host supporting 802.1Q protocol adds a 4-bit 802.1Q tag header after the source address of the former Ethernet frame header when sending packets.

The 4-bit 802.1Q tag header contains a 2-bit Tag Protocol Identifier (TPID) whose value is 8100 and a 2-bit Tag Control Information (TCI). TPID is a new class defined by IEEE to indicate a packet with an 802.1Q tag. Figure 172 describes the detailed contents of an 802.1Q tag header.

Figure 172 802.1Q tag headers



In the figure above, the 3-bit priority field in TCI is 802.1p priority in the range of 0 to 7. The 3 bits specify the precedence of the frame. 8 classes of precedence are used to determine which packet is sent preferentially when the switch is congested.

Table 530 Description on 802.1p priority

CoS (decimal)	CoS (binary)	Description
0	000	best-effort
1	001	background
2	010	spare
3	011	excellent-effort
4	100	controlled-load
5	101	video
6	110	voice
7	111	network-management

The precedence is called 802.1p priority because the related applications of this precedence are defined in detail in the 802.1p specification.

3 Local precedence

Local precedence is the precedence of an outbound queue on a port of the switch. It is in the range of 0 to 7. Each outbound queue has its own local precedence.

Priority of Protocol Packets

Protocol packets carry their own priority. You can perform QoS actions on protocol packets by setting their priorities.

Priority Remark

The priority remark function is to use ACL rules in traffic identification and remark the priority for the packets matching with the ACL rules.

Packet Filter

Packet filter means filtering the service traffic. For example, in the operation of dropping packets, the service traffic matching with the traffic classification rule is

dropped and the other traffic is permitted. The Ethernet switch adopts a complicated traffic classification rule to filter the packets based on much information and to drop these useless, unreliable, and doubtful packets. Therefore, the network security is enhanced.

The two critical steps in the packet filter operation are:

Step1: Classify the inbound packets to the port by the set classification rule.

Step 2: Perform the filter--drop operation on the classified packets.

The packet filter function can be implemented by applying ACL rules on the port. Refer to the description in t"ACL Configuration" on page 637 for detailed configurations.

Rate Limit on Ports

Rate limit on ports is port-based rate limit. It limits the total rate of outbound packets on a port.

TP

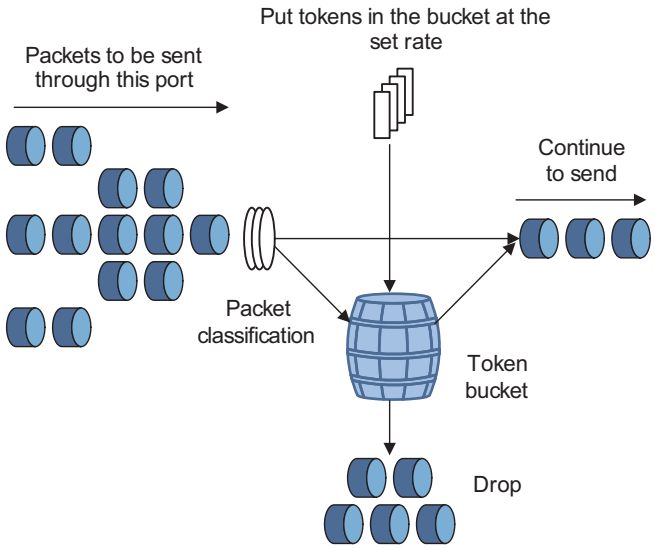
The network will be made more congested by plenty of continuous burst packets if the traffic of each user is not limited. The traffic of each user must be limited in order to make better use of the limited network resources and provide better service for more users. For example, the traffic can only get its committed resources in an interval to avoid network congestion caused by excess bursts.

TP (traffic policing) is a kind of traffic control policy to limit the traffic and its resource usage by supervising the traffic specification. The regulation policy is implemented according to the evaluation result on the premise of knowing whether the traffic exceeds the specification when TP or TS is performed. The token bucket is generally adopted in the evaluation of traffic specification.

Traffic evaluation and the token bucket

The token bucket can be considered as a container with a certain capacity to hold tokens. The system puts tokens into the bucket at the set rate. When the token bucket is full, the extra tokens will overflow and the number of tokens in the bucket stops increasing.

Figure 173 Evaluate the traffic with the token bucket



1 Evaluate the traffic with the token bucket

The evaluation for the traffic specification is based on whether the number of tokens in the bucket can meet the need of packet forwarding. If the number of tokens in the bucket is enough to forward the packets (generally, one token is associated with a 1-bit forwarding authority), the traffic is conforming to the specification, and otherwise the traffic is nonconforming or excess.

When the token bucket evaluates the traffic, its parameter configurations include:

- Average rate: The rate at which tokens are put into the bucket, namely, the permitted average rate of the traffic. It is generally set to committed information rate (CIR).
- Burst size: The capacity of the token bucket, namely, the maximum traffic size that is permitted in every burst. It is generally set to committed burst size (CBS). The set burst size must be bigger than the maximum packet length.

One evaluation is performed on each arriving packet. In each evaluation, if the number of tokens in the bucket is enough, the traffic is conforming to the specification and you must take away some tokens whose number is corresponding to the packet forwarding authority; if the number of tokens in the bucket is not enough, it means that too many tokens have been used and the traffic is excess.

2 Complicated evaluation

You can set two token buckets in order to evaluate more complicated conditions and implement more flexible regulation policies. For example, TP includes 4 parameters:

- CIR
- CBS
- Peak information rate (PIR)
- Excess burst size (EBS)

Two token buckets are used in this evaluation. Their rates of putting tokens into the buckets are CIR and PIR respectively, and their sizes are CBS and EBS respectively (the two buckets are called C bucket and E bucket respectively for short), representing different permitted burst levels. In each evaluation, you can implement different regulation policies in different conditions, including "enough tokens in C bucket", "insufficient tokens in C bucket but enough tokens in E bucket" and "insufficient tokens in both C bucket and E bucket".

TP

The typical application of TP is to supervise the specification of certain traffic into the network and limit it within a reasonable range, or to punish the extra traffic. Therefore, the network resources and the interests of the operators are protected. For example, you can limit HTTP packets within 50% of the network bandwidth. If the traffic of a certain connection is excess, TP can choose to drop the packets or to reset the priority of the packets.

TP is widely used in policing the traffic into the network of internet service providers (ISP).TP can classify the policed traffic and perform pre-defined policing actions according to different evaluation results. These actions include:

- Forward: Forward the packets although the evaluation result is "incompliant".
- Drop: Drop the packets whose evaluation result is "incompliant".
- Remark the DSCP precedence and then forward: Modify the DSCP precedence of the packets whose evaluation result is "incompliant" and then forward them.

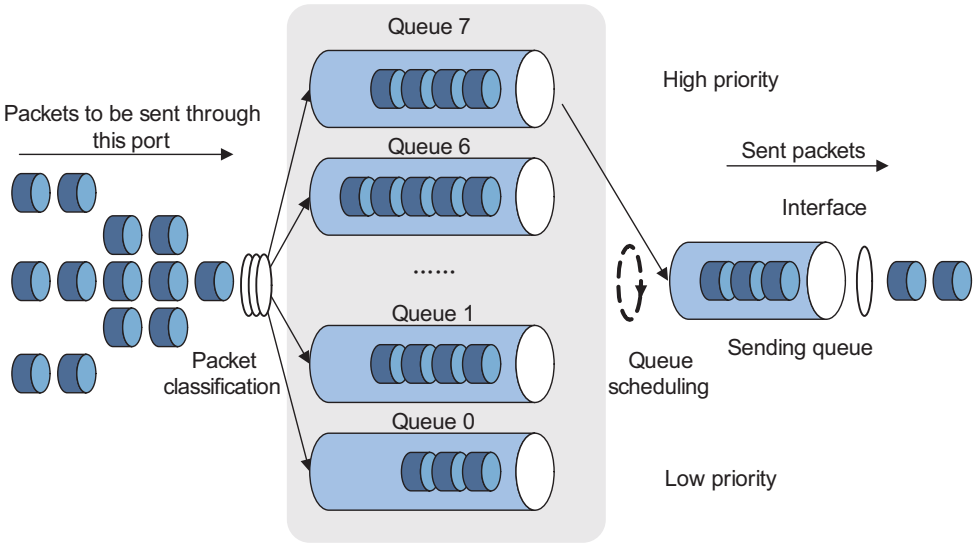
Redirect You can re-specify the forwarding port of packets as required by your own QoS policy.

Queue Scheduling When the network is congested, the problem that many packets compete for resources must be solved, usually in the way of queue scheduling.

In the following section, strict priority (SP) queues and weighted round robin (WRR) queues are introduced.

1 SP queue

Figure 174 Diagram for SP queues



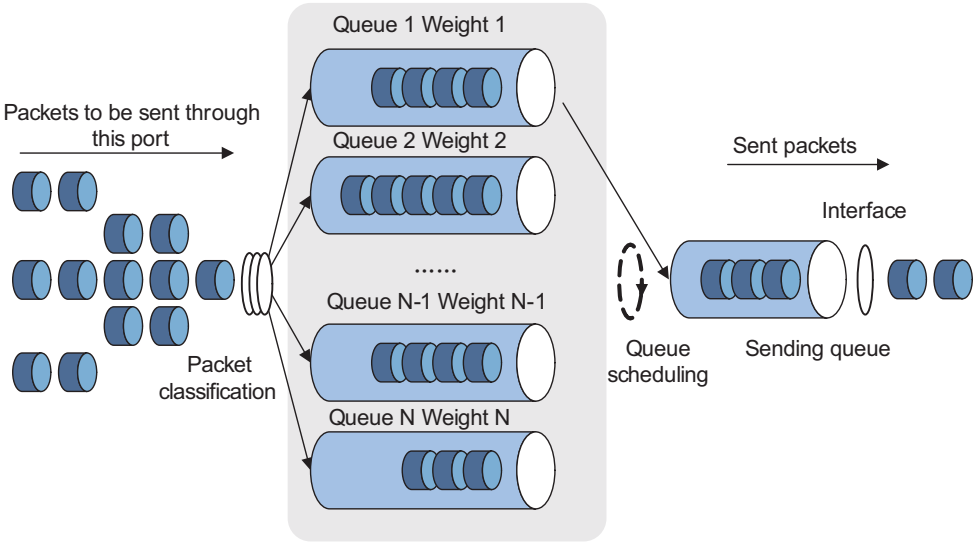
SP queue-scheduling algorithm is specially designed for critical service applications. An important feature of critical services is that they demand preferential service in congestion in order to reduce the response delay. Assume that there are 8 output queues on the port and the preferential queue classifies the 8 output queues on the port into 8 classes, which are queue7, queue6, queue5, queue4, queue3, queue2, queue1, and queue0. Their priorities decrease in order.

In the queue scheduling, SP sends packets in the queue with higher priority strictly following the priority order from high to low. When the queue with higher priority is empty, packets in the queue with lower priority are sent. You can put critical service packets into the queues with higher priority and put non-critical service (such as e-mail) packets into the queues with lower priority. In this case, critical service packets are sent preferentially and non-critical service packets are sent when critical service groups are not sent.

The disadvantage of SP queue is that: if there are packets in the queues with higher priority for a long time in congestion, the packets in the queues with lower priority will be "starved to death" because they are not served.

2 WRR queue

Figure 175 Diagram for WRR



3 WRR queue-scheduling algorithm schedules all the queues in turn and every queue can be assured of a certain service time. Assume there are 8 priority queues on the port. WRR configures a weight value for each queue, which are w7, w6, w5, w4, w3, w2, w1, and w0. The weight value indicates the proportion of obtaining resources. On a 100M port, configure the weight value of WRR queue-scheduling algorithm to 50, 50, 30, 30, 10, 10, 10 and 10 (corresponding to w7, w6, w5, w4, w3, w2, w1, and w0 in order). In this way, the queue with the lowest priority can get 5 Mbps bandwidth at least, and the disadvantage of SP queue-scheduling that the packets in queues with lower priority may not get service for a long time is avoided. Another advantage of WRR queue is that: though the queues are scheduled in order, the service time for each queue is not fixed, that is to say, if a queue is empty, the next queue will be scheduled. In this way, the bandwidth resources are made full use of.

Traffic-based Traffic Statistics

The function of traffic-based traffic statistics is to use ACL rules in traffic identifying and perform traffic statistics on the packets matching with the ACL rules. You can get the statistics of the packets you are interested in through this function.

RED

When congestion is too serious, the switch can adopt the random early detection (RED) algorithm to solve the problem of excessive congestion and avoid global TCP synchronization caused by the tail-drop algorithm.

When packets of one or more TCP connections are dropped at random and the traffic is gradually reduced, packets of other TCP connections can still be sent at a high rate. In this way, packets in a part of connections are sent at a high rate in any case. Thus, the utilization rate of bandwidth is improved.

In the RED algorithm, an upper limit and a lower limit are set for each queue, and it is stipulated that:

- When the queue length is smaller than the lower limit, packets are not dropped.

- When the queue length is bigger than the upper limit, all inbound packets all dropped.
- When the queue length is in the range of the upper limit and the lower limit, the inbound packets are dropped at random. In this case, a number is assigned to each inbound packet and then compared with the drop probability of the current queue. If the number is bigger than the drop probability, the inbound packet is dropped. The longer a queue is, the higher the drop probability is. However, there is a top drop probability.

QoS Supported by the Switch 7750

Table 531 QoS functions supported by the Switch 7750 and related commands

QoS	Description	Related command
Priority mapping	Support only the mapping between 802.1p priority and local queues	**qos cos-local-precedence-map**
Port priority	Supported	**priority** *priority-level*
Priority to be used when a packet enters a queue	Supported	**priority-trust**
TP	Supported	**traffic-limit**
Priority remark	Supported	**traffic-priority**
Redirect	Supported	**traffic-redirect**
Queue scheduling	Support SP and WRR	**queue-scheduler**
Rate limit	Supported	**line-rate**
Bandwidth assurance	Supported	**traffic-bandwidth**
Congestion avoidance	Support the RED operation	**traffic-red**
Traffic statistics	Supported	**traffic-statistic**
Inbound CAR	Supported	**inboundcar** { **enable** | **disable** }
Traffic-based selective QinQ	Supported	**traffic-remark**

Setting Port Priority

If an inbound packet is not VLAN-tagged, the switch will tag the packet with the default VLAN of the port receiving the packet. In this case, the port priority of the port receiving the packet is assigned to the 802.1p priority of the VLAN tag of the packet. In this case, you can set the port priority.

If the inbound packet is VLAN-tagged, the switch does not perform the operation above.

Configuration prerequisites

- The port whose priority is to be configured is specified
- The priority value of the specified port is specified

Configuration procedure

Table 532 Set to use the port priority

Operation	Command	Description
Enter system view	**system-view**	-

Table 532 Set to use the port priority

Operation	Command	Description
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Set the port priority	**priority** *priority-level*	Optional By default, the port priority is 0

Configuration example

- Set the port priority of Ethernet 2/0/1 to 7.

Configuration procedure:

```
<SW7750> system-view
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] priority 7
```

Configuring Priority to Be Used When a Packet Enters an Output Queue

When congestion occurs in the network, queue scheduling is generally adopted to solve the problem that multiple packets compete for resources.

A port of the switch supports eight output queues. The priority of each queue is different, and packets in the queue with higher priority are sent preferentially. The switch puts a packet into the corresponding queue according to the DSCP precedence, IP precedence, 802.1p priority or local precedence of the packet. The mapping relationship between precedence values and queues are shown in Table 533, Table 534, Table 535, and Table 536.

Table 533 The mapping relationship between the 802.1p priority values and queues

802.1p priority	Queue
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

Table 534 The mapping relationship between the local precedence values and queues

Local precedence	Queue
0	0
1	1
2	2
3	3
4	4
5	5
6	6

Table 534 The mapping relationship between the local precedence values and queues

Local precedence	Queue
7	7

Table 535 The mapping relationship between IP precedence values and queues

IP precedence	Queue
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Table 536 The mapping relationship between DSCP precedence values and queues

DSCP precedence value	Name of type-A I/O Module	Name of non-type-A I/O Module	Queue
0 to 7	be(0)	be(0)	0
8 to 15	cs1(8), af1(10)	cs1(8), af11(10), af12(12), af13(14)	1
16 to 23	cs2(16), af2(18)	cs2(16), af21(18), af22(20), af23(22)	2
24 to 31	cs3(24), af3(26)	cs3(24), af31(26), af32(28), af33(30)	3
32 to 39	cs4(32), af4(34)	cs4(32), af41(34) , af42(36) , af43(38)	4
40 to 47	cs5(40), ef(46)	cs5(40), ef(46)	5
47 to 55	cs6(48)	cs6(48)	6
56 to 63	cs7(56)	cs7(56)	7

Configuring Priority to Be Used When a Packet Enters an Output Queue

You can select the corresponding priority as the basis for a packet to enter an output queue on a port as required.

Configuration prerequisites

The priority to be used when a packet enter a queue is specified.

Configuration procedure

Table 537 Configure the priority to be used when a packet enters a queue

Operation	Command	Description
Enter system view	**system-view**	-
Configure the priority to be used when a packet enters an output queue	**priority-trust** { **dscp** | **ip-precedence** | **cos** | **local-precedence** }	Required By default, the local precedence is used when a packet enter an output queue

Configuration example

Configure to use the DSCP precedence when a packet enters an output queue

```
<SW7750> system-view
[SW7750] priority-trust dscp
```

Configuring the Mapping Relationship between 802.1p Priority Values and Queues

You can modify the mapping relationship between 802.1p priority values and local precedence values to modify the mapping relationship between 802.1p priority values and output queues.

Configuration prerequisites

The mapping relationship between 802.1p priority values and local precedence values and the default mapping table are well known.

Configuration procedure

Table 538 Configure the COS-to-local-precedence mapping table

Operation	Command	Description
Enter system view	**system-view**	-
Configure the COS-to-local-precedence mapping table	**qos cos-local-precedence-map** *cos0-map-local-prec cos1-map-local-prec cos2-map-local-prec cos3-map-local-prec cos4-map-local-prec cos5-map-local-prec cos6-map-local-prec cos7-map-local-prec*	Optional
Display the mapping table	**display qos cos-local-precedence-map**	You can execute the **display** command in any view

Configuration example

- Configure the 802.1p-to-local-precedence as follows: 0 to 2, 1 to 3, 2 to 4, 3 to 1, 4 to 7, 5 to 0, 6 to 5 and 7 to 6.
- Display the configuration.

Configuration procedure:

```
<SW7750> system-view
[SW7750] qos cos-local-precedence-map 2 3 4 1 7 0 5 6
[SW7750] display qos cos-local-precedence-map
 cos-local-precedence-map:
              cos :       0      1      2      3      4      5      6      7
------------------------------------------------------------------------------
 local-precedence :       2      3      4      1      7      0      5      6
```

Configuring Priority Remark

Refer to "Priority Remark" on page 660 for the introduction to priority remark.

Priority remark can be implemented in the following ways:

- Through TP (only non-type-A I/O Modules support this function). When configuring TP, you can define the action of remarking the DSCP precedence for the packets exceeding the traffic limit. Refer to "Configuration Procedure of TP" on page 672.

- Through the **traffic-priority** command. Refer to the following description in this section.

Configuration Prerequisites

- ACL rules used for traffic identifying are defined. Refer to "Choosing ACL Mode for Traffic Flows" on page 639 for defining ACL rules.
- The type and value of the precedence that the packets matching with ACL rules are remarked are specified
- The ports which need this configuration are specified

Configuration Procedure

Table 539 Configure priority remark

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Enter QoS view	**qos**	-
Use ACL rules in traffic identifying and specify a new precedence for the packet matching with the ACL rules	**traffic-priority** { **inbound** | **outbound** } *acl-rule* [**system-index** *system-index*] { { **dscp** *dscp-value* | **ip-precedence** *pre-value* } | **local-precedence** *pre-value* }*	Required Type-A I/O Modules support this command
	traffic-priority inbound *acl-rule* [**system-index** *system-index*] { { **dscp** *dscp-value* | **ip-precedence** *pre-value* } | { **cos** *cos* | **local-precedence** *pre-value* } }*	Optional Non-type-A I/O Modules support this command
Display the parameter configurations of priority remark	**display qos-interface** [*interface-type interface-number*] **traffic-priority**	Optional You can execute the **display** command in any view
Display all the QoS settings of the port	**display qos-interface** [*interface-type interface-number*] **all**	

acl-rule: Applied ACL rules which can be the combination of various ACL rules. The way of combination is described in the following table:

Table 540 Type-A I/O Modules' ways of applying combined ACLs

ACL combination	Form of the acl-rule argument
Apply all the rules in an IP ACL separately	**ip-group** { *acl-number* | *acl-name* }
Apply a rule in an IP ACL separately	**ip-group** { *acl-number* | *acl-name* } **rule** *rule-id*
Apply all the rules in a Link ACL separately	**link-group** { *acl-number* | *acl-name* }
Apply a rule in a Link ACL separately	**link-group** { *acl-number* | *acl-name* } **rule** *rule-id*

Table 541 Non-type-A I/O Modules' ways of applying combined ACLs

ACL combination	Form of the acl-rule argument
Apply all the rules in an IP ACL separately	**ip-group** { *acl-number* | *acl-name* }
Apply a rule in an IP ACL separately	**ip-group** { *acl-number* | *acl-name* } **rule** *rule-id*
Apply all the rules in a Link ACL separately	**link-group** { *acl-number* | *acl-name* }
Apply a rule in a Link ACL separately	**link-group** { *acl-number* | *acl-name* } **rule** *rule-id*
Apply all the rules in a user-defined ACL separately	**user-group** { *acl-number* | *acl-name* }
Apply a rule in a user-defined ACL separately	**user-group** { *acl-number* | *acl-name* } **rule** *rule-id*
Apply a rule in an IP ACL and a rule in a Link ACL at the same time	**ip-group** { *acl-number* | *acl-name* } **rule** *rule-id* **link-group** { *acl-number* | *acl-name* } **rule** *rule-id*

Configuration Example

- Ethernet 2/0/1 of the switch is accessed into the 10.1.1.1/24 network segment
- Remark the DSCP precedence of the traffic from the 10.1.1.1/24 network segment to 56

Configuration procedure:

```
<SW7750> system-view
[SW7750] acl number 2000
[SW7750-acl-basic-2000] rule permit source 10.1.1.1 0.0.0.255
[SW7750-acl-basic-2000] quit
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] qos
[SW7750-qosb-Ethernet2/0/1] traffic-priority inbound ip-group 2000 dscp 56
```

Configuring Rate Limit on Ports

Configuration Prerequisites

- The ports where rate limit is to be performed is specified
- The target rate is specified

Configuration Procedure

Table 542 Configure rate limit on ports

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Enter QoS view	**qos**	-
Configure port-based rate limit	**line-rate** [**kbps**] *target-rate*	Required
Display the precedence of the protocol packet	**display protocol-priority**	Optional You can execute the **display** command in any view

Only non-type-A I/O Modules support port-based rate limit.

Configuration Example

- Set rate limit on GigabitEthernet 2/0/1 of the switch
- Limit the rate to 10 Mbps.

Configuration procedure:

```
<SW7750> system-view
[SW7750] interface GigabitEthernet 2/0/1
[SW7750-GigabitEthernet2/0/1] qos
[SW7750-qosb-GigabitEthernet2/0/1] line-rate 10
```

Configuring TP

Refer to "TP" on page 661 for the introduction to TP.

Configuration Prerequisites

- ACL rules used for traffic identifying are defined. Refer to "Choosing ACL Mode for Traffic Flows" on page 639 for defining ACL rules
- The limit rate for TP, the actions for the packets within the specified traffic and the actions for the packets beyond the specified traffic have been specified.
- The ports that needs this configuration is specified

Configuration Procedure of TP

Table 543 Configure TP

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Enter QoS view	**qos**	-
Configure traffic-based TP	**traffic-limit** { **inbound** | **outbound** } *acl-rule* [**system-index** *system-index*] *target-rate*	Required Type-A I/O Modules support this command.
	traffic-limit inbound *acl-rule* [**system-index** *system-index*] [**kbps**] *target-rate* [**exceed** *action*]	Required Non-type-A I/O Modules support this command.
Display the parameters for traffic policing	**display qos-interface** [*interface-type interface-number*] **traffic-limit**	Optional You can execute the **display** command in any view.
Display all the QoS settings of the port	**display qos-interface** [*interface-type interface-number*] **all**	

acl-rule: Applied ACL rules which can be the combination of various ACL rules. Type-A I/O Modules' ways of combinations are described in Table 540, and non-type-A I/O Modules' ways of combination is described in Table 541.

- *TP configuration is effective only for the ACL rules whose actions are **permit**.*

- *When a switch is connected to a RADIUS server, if the switch does not support the inbound TP or outbound TP configured on the RADIUS server, the TP configuration will be ignored on the switch.*

Configuration Example

- GigabitEthernet 2/0/1 of the switch is accessed to the 10.1.1.1/24 network segment
- Perform TP on the packets from the 10.1.1.1/24 network segment and the rate of TP is set to 128 kbps
- The packets beyond the specified traffic are forwarded after their DSCP precedence is marked as 56

Configuration procedure:

```
<SW7750> system-view
[SW7750-acl-basic-2000] rule permit source 10.1.1.1 0.0.0.255
[SW7750-acl-basic-2000] quit
[SW7750] interface GigabitEthernet 2/0/1
[SW7750-GigabitEthernet2/0/1] qos
[SW7750-qosb-GigabitEthernet2/0/1] traffic-limit inbound ip-group 20
00 kbps 128 exceed remark-dscp 56
```

Configuring Redirect

Refer to "Redirect" on page 663 for the introduction to redirect.

Configuration Prerequisites

- ACL rules used for traffic identifying are defined. Refer to "Choosing ACL Mode for Traffic Flows" on page 639 for defining ACL rules
- The port that the packets are redirected to is specified
- The ports that needs this configuration are specified

Configuration Procedure

Table 544 Configure redirect

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Enter QoS view	**qos**	-
Configure redirect	**traffic-redirect inbound** *acl-rule* [**system-index** *system-index*] { **cpu** | **interface** *interface-type interface-number* }	Required
Display the parameters for traffic redirect	**display qos-interface** [*interface-type interface-number*] **traffic-redirect**	Optional You can execute the **display** command in any view.
Display all the QoS settings of the port	**display qos-interface** [*interface-type interface-number*] **all**	

acl-rule: Applied ACL rules which can be the combination of various ACL rules. The way of combination is described in Table 541.

- *Only non-type-A I/O Modules support the traffic redirect configuration.*
- *The redirect configuration is effective only for the ACL rules whose actions are **permit**.*
- *Packets redirected to CPU will not be forwarded normally.*

Configuration Example

- Ethernet 2/0/1 of the switch is accessed into the 10.1.1.1/24 network segment.
- Redirect all the traffic from the 10.1.1.1/24 network segment to Ethernet 2/0/7.

Configuration procedure:

```
<SW7750> system-view
[SW7750] acl number 2000
[SW7750-acl-basic-2000] rule permit source 10.1.1.1 0.0.0.255
[SW7750-acl-basic-2000] quit
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] qos
[SW7750-qosb-Ethernet2/0/1] traffic-redirect inbound ip-group 2000 i
nterface Ethernet 2/0/7
```

Configuring Queue-scheduling

Refer to "Queue Scheduling" on page 663 for the introduction to queue scheduling.

Configuration Prerequisites

- The queue-scheduling algorithm is specified.
- The ports that need this configuration are specified.

Configuration Procedure

Table 545 Configure queue scheduling

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Enter QoS view	**qos**	-
Configure the queue scheduling mode	**queue-scheduler** { **rr** | **strict-priority** | **wrr** *queue1-weight queue2-weight queue3-weight queue4-weight queue5-weight queue6-weight queue7-weight queue8-weight* }	Required By default, the SP queue scheduling algorithm is adopted.
Display the parameters for traffic redirect	**display qos-interface** [*interface-type interface-number*] **queue-scheduler**	Optional You can execute the **display** command in any view.
Display all the QoS settings on the port	**display qos-interface** [*interface-type interface-number*] **all**	

Only non-type-A I/O Modules support the configuration for queue scheduling mode.

Configuration Example

- The switch adopts the WRR queue scheduling algorithm, and the weight values of outbound queues are 10, 5, 10, 10, 5, 10, 5, and 10 respectively;
- Display the configuration.

Configuration procedure:

```
<SW7750> system-view
[SW7750] interface GigabitEthernet 2/0/1
[SW7750-GigabitEthernet2/0/1] qos
[SW7750-qosb-GigabitEthernet2/0/1] queue-scheduler wrr 10 5 10 10 5 10 5 10
[SW7750-qosb-GigabitEthernet2/0/1] display qos-interface GigabitEthernet 2/0/1 qu
eue-scheduler

GigabitEthernet2/0/1:
 Queue scheduling mode: weighted round robin
 weight of queue 1: 10
 weight of queue 2: 5
 weight of queue 3: 10
 weight of queue 4: 10
 weight of queue 5: 5
 weight of queue 6: 10
 weight of queue 7: 5
 weight of queue 8: 10
 COS configuration:
  Config (max queues): 8
  Schedule mode: weighted round-robin
  Weighting (in packets):
    COSQ 0 = 10 packets
    COSQ 1 = 5 packets
    COSQ 2 = 10 packets
    COSQ 3 = 10 packets
    COSQ 4 = 5 packets
    COSQ 5 = 10 packets
    COSQ 6 = 5 packets
    COSQ 7 = 10 packets
  Egress port queue statistics(in bytes):
    Priority    CosQ        Threshold   Count       Used(%):
    0           2           18432       0           0
    1           0           2560        0           0
    2           1           2560        0           0
    3           3           2560        0           0
    4           4           2560        0           0
    5           5           2560        0           0
    6           6           2560        0           0
    7           7           2560        0           0
  common queue statistics(in bytes):
                            49152       0           0
```

Configuring Congestion Avoidance

When congestion happens, the switch will drop packets as soon as possible to release queue resources and try not to put packets into high-delay queues in order to eliminate congestion. The switch adopts the RED algorithm for congestion avoidance.

Configuration Prerequisites

- The indexes of queues to be dropped at random, the queue length that starts the drop action, the queue length that causes all the packets to be dropped and the drop probability are specified
- The ports that need this configuration are specified

Configuration Procedure

Table 546 Configure RED parameters

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Enter QoS view	**qos**	-
Configure parameters for the RED algorithm	**traffic-red outbound** *acl-rule* [**system-index** *system-index*] *qstart qstop probability*	Required The maximum available bandwidth must be no smaller than the minimum assured bandwidth.
Display the parameters for the RED configuration	**display qos-interface** [*interface-type interface-number*] **traffic-red**	Optional You can execute the **display** command in any view.
Display all the QoS settings on the port	**display qos-interface** [*interface-type interface-number*] **all**	

acl-rule: Applied ACL rules which can be the combination of various ACL rules. The way of combination is described in Table 541.

- *Only type-A I/O Modules support the configuration above.*
- *Only the rules with the **permit** action can be properly applied to the hardware.*

Configuration Example

- Ethernet 2/0/1 is accessed to the network segment 10.1.1.1/24.
- Perform the RED queue scheduling algorithm for all the inbound traffic from 10.1.1.1/24
- Set the parameters as follows: the packets are dropped at random when the queue length exceeds 64 KB, all packets are dropped when the queue length exceeds 128 KB, and the drop probability is 20%.

Configuration procedure:

```
<SW7750> system-view
[SW7750] acl number 2000
[SW7750-acl-basic-2000] rule permit source 10.1.1.1 0.0.0.255
[SW7750-acl-basic-2000] quit
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] qos
[SW7750-qoss-Ethernet2/0/1] traffic-red outbound ip-group 2000 64 128 20
```

Configuring Traffic Statistics

Refer to "Traffic-based Traffic Statistics" on page 665 for the introduction to traffic statistics.

Configuration Prerequisites

- ACL rules used for traffic identifying are defined. Refer to "Choosing ACL Mode for Traffic Flows" on page 639 for defining ACL rules
- The ports that needs this configuration are specified

Configuration Procedure of Traffic Statistics

Table 547 Configure traffic statistics

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Enter QoS view	**qos**	-
Use the ACL rules in traffic identifying and perform traffic statistics on the packets matching with the ACL rules.	**traffic-statistic** { **inbound** | **outbound** } *acl-rule* [**system-index** *system-index*]	Required Type A I/O Modules support this command.
	traffic-statistic inbound *acl-rule* [**system-index** *system-index*]	Required Non-type-A support this command
Display the traffic statistics.	**display qos-interface** [*interface-type interface-number*]	Optional You can execute the **display** command in any view
Display all the QoS settings of the port	**display qos-interface** [*interface-type interface-number*] **all**	

acl-rule: Applied ACL rules which can be the combination of various ACL rules. Type-A I/O Modules' way of combination is described in Table 540, and non-type-A I/O Modules' way of combination is described in Table 541.

Clearing Traffic Statistics Information

Table 548 Clear traffic statistics information

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Enter QoS view	**qos**	-
Clear the statistics of the traffic matching with the specified ACL rules	**reset traffic-statistic** { **inbound** | **outbound** } *acl-rule*	Required Type-A I/O Modules support this command.
	reset traffic-statistic inbound *acl-rule*	Required Non-type-A I/O Modules support this command.

acl-rule: Applied ACL rules which can be the combination of various ACL rules. Type-A I/O Modules' way of combination is described in Table 540, and non-type-A I/O Modules' way of combination is described in Table 541.

Configuration Example

- Ethernet 2/0/1 of the switch is accessed into the 10.1.1.1/24 network segment
- Perform traffic statistics on packets from the 10.1.1.1/24 network segment

Configuration procedure:

```
<SW7750> system-view
[SW7750] acl number 2000
[SW7750-acl-basic-2000] rule permit source 10.1.1.1 0.0.0.255
[SW7750-acl-basic-2000] quit
```

```
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] qos
[SW7750-qosb-Ethernet2/0/1] traffic-statistic inbound ip-group 2000
```

Configuring Assured Bandwidth

The function of assured bandwidth is to provide the maximum available bandwidth and minimum assured bandwidth for the specified traffic to get the corresponding service.

Configuration Prerequisites

- ACL rules used for traffic identifying are defined. Refer to "Choosing ACL Mode for Traffic Flows" on page 639 for defining ACL rules
- The parameters for the assured bandwidth are specified
- The ports that need this configuration are specified

Configuration Procedure

Table 549 Configure assured bandwidth

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Enter QoS view	**qos**	-
Enable ACLs to identify traffic and provide assured bandwidth for the specified traffic	**traffic-bandwidth outbound** *acl-rule* [**system-index** *system-index*] *min-guaranteed-bandwidth max-guaranteed-bandwidth weight*	Required The maximum available bandwidth must be no smaller than the minimum assured bandwidth.
Display the traffic statistics	**display qos-interface** [*interface-type interface-number*] **traffic-bandwidth**	Optional You can execute the **display** command in any view.
Display all the QoS settings on the port	**display qos-interface** [*interface-type interface-number*] **all**	

acl-rule: Applied ACL rules which can be the combination of various ACL rules. Type-A I/O Modules' way of combination is described in Table 540, and non-type-A I/O Modules' way of combination is described in Table 541.



- *Only type-A I/O Modules support the configuration above.*
- *Only the rules with the **permit** action can be properly applied to the hardware.*

Configuration Example

- Ethernet 2/0/1 of the switch is accessed into the network segment 10.1.1.1/24.
- Enable the function of assured bandwidth for traffic from the network segment 10.1.1.1/24.
- Set the parameters as follows: the minimum assured bandwidth is 64 kbps, the maximum available bandwidth is 128 kbps, and the weight of bandwidth is 50.

Configuration procedure:

```
<SW7750> system-view
[SW7750] acl number 2000
[SW7750-acl-basic-2000] rule permit source 10.1.1.1 0.0.0.255
[SW7750-acl-basic-2000] quit
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] qos
[SW7750-qoss-Ethernet2/0/1] traffic-bandwidth outbound ip-group 2000 64 128 50
```

Configuring Bidirectional CAR

You can enable or disable bidirectional CAR.

With bidirectional CAR enabled, the switch considers an ACL rule applied to different ports as different rules. As a result, an applied rule can occupy multiple entries. If you enable CAR for traffic matching a certain rule on multiple ports, the switch provides the specified bandwidth for the traffic matching the CAR rule on a per-port basis.

With bidirectional CAR disabled, the switch considers an ACL rule applied to different ports as the same rule. As a result, an applied rule occupies only one entry. If you enable CAR for traffic matching a certain rule on multiple ports, the switch provides the specified bandwidth for all the traffic matching the CAR rule on these ports to share.

Suppose you want to allocate 2 Mbps of CAR bandwidth for the incoming traffic matching ACL rule 0 and enable CAR on two ports with the **traffic-limit** command.

- If bidirectional CAR is enabled, each port guarantees 2 Mbps of bandwidth for its incoming traffic matching ACL rule 0.
- If bidirectional CAR is disabled, the switch guarantees 2 Mbps of bandwidth for the traffic matching ACL rule 0 received on the two ports.

Configuration Procedure

Table 550 Configure bidirectional CAR

Operation	Command	Description
Enter system view	**system-view**	-
Enable or disable bidirectional CAR	**inboundcar** { **enable** | **disable** }	Required Disabled by default.



This command applies to only type-A I/O Modules. To make the configuration take effect, reboot the switch.

Configuration Example

- Enable bidirectional CAR

Configuration procedure:

```
<SW7750> system-view
[SW7750] inboundcar enable
```

Configuring Traffic-Based Selective QinQ

QinQ is to encapsulate the VLAN tags of the private network in the VLAN tags of the public network in order that the packets are transmitted through the backbone network of the carrier (also called public network). The traffic-based

selective QinQ function can tag a packet with external VLAN tags according to the ACL rule that the packets matches on the inbound port.

The traffic-based selective QinQ function is configured on the hybrid port of the edge device connecting the user device to the carrier's network.

Configuration Prerequisites

- ACL rules used for traffic identifying are defined. Refer to "Choosing ACL Mode for Traffic Flows" on page 639 for defining ACL rules.
- ID of the external VLAN tag is specified
- The ports that needs this configuration are specified

Configuration Procedure

Table 551 Configure traffic-based selective QinQ

Operation	Command	Description
Enter system view	**system-view**	-
Create a VLAN	**vlan** *vlan-id*	The *vlan-id* argument is the ID of external VLAN tag.
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Set the port type to hybrid	**port link-type hybrid**	-
Add the hybrid port to the specified VLAN	**port hybrid vlan** *vlan-id* { **tagged** | **untagged** }	*vlan-id* is the ID of out-layer VLAN Tag
Enable the QinQ feature in the port view	**vlan-vpn enable**	Required
Enter QoS view	**qos**	-
Enable the ACL rule for traffic identifying and tag the matching packets with external VLAN tags	**traffic-remark inbound** *acl-rule* [**system-index** *system-index*] **remark-vlan** *vlan-id* **uplink** *interface-type interface-number* [**untagged**]	Required
Display the traffic statistics	**display qos-interface** [*interface-type interface-number*] **traffic-remark**	Required You can execute the **display** command in any view
Display all the QoS settings on the port	**display qos-interface** [*interface-type interface-number*] **all**	

acl-rule: Applied ACL rules which can be the combination of various ACL rules. The way of combination is described in Table 541.



CAUTION:

- *Execute the **vlan-vpn enable** command in the corresponding port view before executing the **traffic-remark** command.*
- *The traffic-based selective QinQ function is generally configured on the hybrid port of the edge device connecting the user device to the carrier's network.*
- *QinQ is mutually exclusive with Voice VLAN. That is, you cannot configure both features on the same port.*
- *The port on which the traffic-based selective QinQ function is configured and the specified uplink port cannot be in the same aggregation group.*

- *Type-A, 3C16863, and 3C16862 I/O Modules do not support the traffic-based selective QinQ function.*

Configuration Example

- GigabitEthernet 2/0/1 of the switch is accessed to the 10.1.1.1/24 network segment
- Tag all the packets from the 10.1.1.1/24 network segment with external VLAN tags to implement the traffic-based selective QinQ function

Configuration procedure:

```
<SW7750> system-view
[SW7750] vlan 25
[SW7750-vlan25] quit
[SW7750] acl number 2000
[SW7750-acl-basic-2000] rule permit source 10.1.1.1 0.0.0.255
[SW7750-acl-basic-2000] quit
[SW7750] interface GigabitEthernet2/0/1
[SW7750-GigabitEthernet2/0/1] port link-type hybrid
[SW7750-GigabitEthernet2/0/1] port hybrid vlan 25 untagged
[SW7750-GigabitEthernet2/0/1] vlan-vpn enable
[SW7750-GigabitEthernet2/0/1] qos
[SW7750-qosb-GigabitEthernet2/0/1] traffic-remark inbound ip-group 2
000 remark-vlan 25 uplink GigabitEthernet 2/0/2
```

QoS Configuration Example

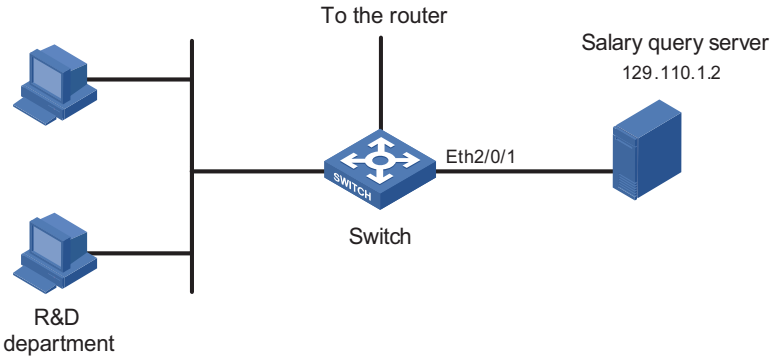
Configuration Example of TP and Rate Limit on the Port

Network requirement

The enterprise network interworks all the departments through the ports of the Ethernet switch. The salary query server of the financial department is accessed through Ethernet 2/0/1 whose subnet address is 129.110.1.2. The network requirements are to limit the average rate of outbound traffic within 640 kbps and set the precedence of packets exceeding the specification to 4.

Network diagram

Figure 176 Network diagram for TP and rate limit configuration



Configuration procedure

Only the commands related with QoS/ACL configurations are listed in the following configurations.

1 Define the outbound traffic of the salary query server

Enter ACL 3000 view.

```
<SW7750> system-view
[SW7750] acl number 3000
```

Define ACL 3000 rules.

```
[SW7750-acl-adv-3000] rule 1 permit ip source 129.110.1.2 0 destination any
[SW7750-acl-adv-3000] quit
```

2 Limit the outbound traffic of the salary query server

Limit the average rate of outbound traffic within 640 kbps and set the precedence of packets exceeding the specification to 4.

```
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] qos
[SW7750-qosb-Ethernet2/0/1] traffic-limit inbound ip-group 3000 640
exceed remark-dscp 4
```

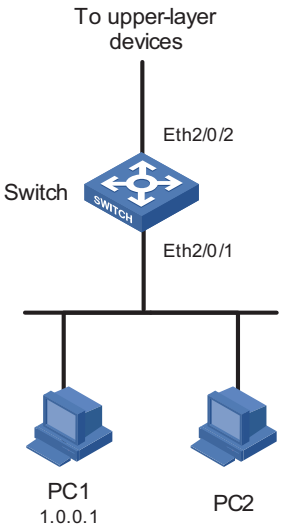
Configuration Example of Priority Remark

Network requirements

Mark ef on the packets that PC1 whose IP address is 1.0.0.2 sends from 8:00 to 18:00 every day to provide the basis of precedence for the upper-layer devices.

Network diagram

Figure 177 Network diagram for priority remark configuration



Configuration procedure

1 Define the time range from 8:00 to 18:00

Define the time range

```
<SW7750> system-view
[SW7750] time-range test 8:00 to 18:00 daily
```

2 Define the traffic rules of PC packets

Enter number-identification-based basic ACL view identified.

```
[SW7750] acl number 2000
[SW7750-acl-basic-2000] rule 0 permit source 1.0.0.1 0 time-range test
[SW7750-acl-basic-2000] quit
```

3 Remark ef precedence on the packets that PC1 sends

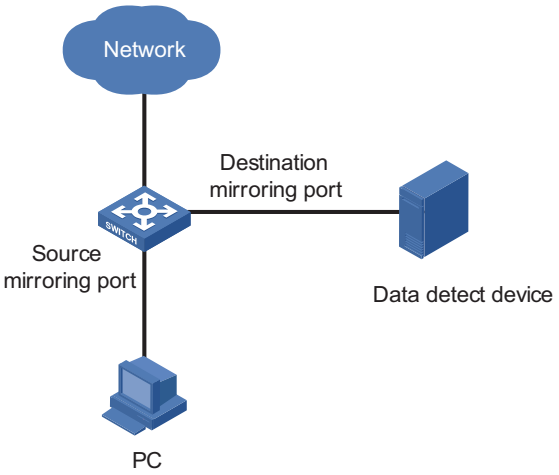
```
[SW7750] interface Ethernet 2/0/1
[SW7750-Ethernet2/0/1] qos
[SW7750-qosb-Ethernet2/0/1] traffic-priority inbound ip-group 2000 dscp ef
```

62 MIRRORING CONFIGURATION

Overview

Mirroring refers to the process of copying packets that meet the specified rules to a destination port. Generally, a destination port is connected to a data detect device, which you can use to analyze the mirrored packets for monitoring and troubleshooting the network. On the other hand, you can also mirror packets to LS81VSNP and LS82VSNP to perform statistics and accounting about the traffic for the users online.

Figure 178 Mirroring



Local Port Mirroring

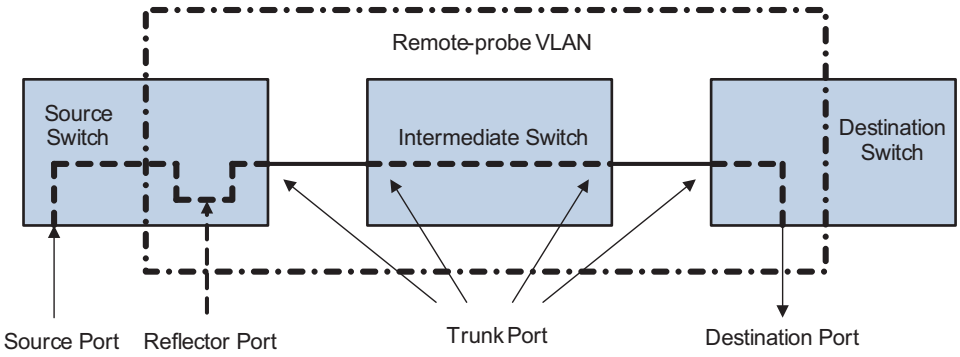
Port mirroring refers to the process of copying the packets received or sent by the specified port to the specified local port.

Remote Port Mirroring

Remote port mirroring eliminates the limitation that the source port and the destination port must be located on the same switch. This feature makes it possible for the source port and the destination port to be located on different devices in the network, and facilitates the network administrator to manage remote switches.

The application of remote port mirroring is illustrated in the following figure:

Figure 179 Remote port mirroring application



There are three types of switches with remote port mirroring enabled.

- Source switch: The switch to which the monitored port belongs. The source switch copies the mirrored traffic flows to the remote-probe VLAN, and then through Layer 2 forwarding, the mirrored flows are sent to an intermediate switch or destination switch.
- Intermediate switch: Switches between the source switch and destination switch on the network. An intermediate switch forwards mirrored flows to the next intermediate switch or the destination switch. Circumstances can occur where no intermediate switch is present, if a direct connection exists between the source and destination switches.
- Destination switch: The switch to which the destination port for remote mirroring belongs. It forwards mirrored flows it received from the remote-probe VLAN to the monitoring device through the destination port.

Table 552 describes how the ports on various switches are involved in the mirroring operation.

Table 552 Ports involved in the mirroring operation

Switch	Ports involved	Function
Source switch	Source port	Port to be mirrored; copy user data packets to the specified reflector port through local port mirroring. There can be more than one source port.
	Reflector port	Receive user data packets that are mirrored on a local port.
	Relay port	Send mirrored packets to the intermediate switch or the destination switch. You must set the port as a trunk port and specify the port to permit packets of remote-probe VLANs.
Intermediate switch	Relay port	Send mirrored packets to the destination switch. Two relay ports are necessary for the intermediate switch to be connected to devices that are connected to the source switch and the destination switch. You must set the port as a trunk port and specify the port to permit packets of remote-probe VLANs.

Table 552 Ports involved in the mirroring operation

Switch	Ports involved	Function
Destination switch	Relay port	Receive remote mirrored packets. You must set the port as a trunk port and specify the port to permit packets of remote-probe VLANs.
	Destination port	Monitor remote mirrored packets

To implement remote port mirroring, you need to define a special VLAN, called remote-probe VLAN, on all the three types of switches. In this VLAN, no normal data but only mirrored packets are transmitted. All mirrored packets will be transferred to the specified port of the destination switch from the source switch through this VLAN. Thus, the destination switch can monitor the packets sent from the ports of the remote source switch. remote-probe VLAN requires that:

- It is recommended that you configure all relay ports in the remote-probe VLAN to be trunk ports.
- The default VLAN and management VLAN cannot be configured as remote-probe VLAN.
- Required configurations are performed to ensure Layer 2 connectivity between the source and destination switches over the remote-probe VLAN.

⚠ ***CAUTION:*** *To ensure the normal packet mirroring, you are not recommended to perform any of the following operations on the remote-probe VLAN*

- *Configuring a source port to the remote-probe VLAN that is used by the local mirroring group;*
- *Configuring a Layer 3 interface for the remote-probe VLAN;*
- *Carrying other protocol packets or service packets;*
- *Using remote-probe VLAN as a special type of VLAN, such as voice VLAN or protocol VLAN;*
- *Configuring other VLAN-related functions.*

Local Traffic Mirroring

Traffic mirroring maps traffic flows that match specific ACLs to the specified local port for packet analysis and monitoring. Before configuring traffic mirroring, you need to define ACLs required for flow identification.

Remote Traffic Mirroring

Remote traffic mirroring copies traffic flows that match specific ACLs to the reflector port of the specified mirroring group. Then, after corresponding configurations of remote port mirroring, the matching traffic flows are finally copied to the specified ports of other switches. Similar to configuring local traffic mirroring, you need to define ACLs required for flow identification first. Otherwise, you need to complete all configurations of remote port mirroring (except the configuration of source port for mirroring).

Mirroring to Local I/O Module

Mirroring to local I/O Module (including LS81VSNP and LS82VSNP) means copying the packets received or sent on the specified port on the specified I/O Module to the specified local I/O Module.

Mirroring Supported by the Switch 7750

Table 553 Mirroring functions supported by the Switch 7750 and related command

Function	Description	Related command	Related section
Mirroring	Support local port mirroring	**mirroring-group** **mirroring-group mirroring-port** **mirroring-group monitor-port** **monitor-port** **mirroring-port**	"Configuring Local Port Mirroring" on page 688
	Support remote port mirroring	**mirroring-group** **mirroring-group mirroring-port** **mirroring-group monitor-port** **mirroring-group reflector-port** **mirroring-group remote-probe vlan** **remote-probe vlan enable**	"Configuring Remote Port Mirroring" on page 690
	Support traffic mirroring	**monitor-port** **mirrored-to**	"Configuring Local Traffic Mirroring" on page 696
	Support remote traffic mirroring	**mirroring-group** **mirroring-group monitor-port** **mirroring-group reflector-port** **mirroring-group remote-probe vlan** **remote-probe vlan enable** **mirrored-to inbound** *acl-rule* [**system-index**] { **interface** *interface-type interface-number* **reflector** | **mirroring-group** *group-id* }	"Configuring Remote Traffic Mirroring" on page 697
	Support mirroring to local I/O Module	**mirroring-group** **mirroring-group mirroring-slot** **mirroring-group monitor-slot** **mirroring-group mirroring-port**	"Configuring Mirroring to Local I/O Module" on page 701

Mirroring Configuration

For mirroring features, see "Overview" on page 685.

Configuring Local Port Mirroring

Configuration prerequisites

- The source port is specified and whether the packets to be mirrored are inbound or outbound is specified.
- The destination port is specified.

Configuring port mirroring in Ethernet port view

Table 554 Configure port mirroring in Ethernet port view

Operation	Command	Description
Enter system view	**system-view**	-

Table 554 Configure port mirroring in Ethernet port view

Operation	Command	Description
Create a local port mirroring group	**mirroring-group** *group-id* **local**	Required
Enter Ethernet port view of the destination port	**interface** *interface-type interface-number*	-
Define the current port as the destination port	**mirroring-group** *group-id* **monitor-port**	Required LACP must be disabled on the mirroring destination port and you are recommended to disable STP on the mirroring destination port.
Exit current view	**quit**	-
Enter Ethernet port view of the source port	**interface** *interface-type interface-number*	-
Configure the source port and specify the direction of the packets to be mirrored	**mirroring-group** *group-id* **mirroring-port** { **both** | **inbound** | **outbound** }	Required
Display parameter settings of the local port mirroring group	**display mirroring-group** { **all** | **local** }	Required This command can be executed in any view.

Configuring local port mirroring in system view

Table 555 Configure local port mirroring in system view

Operation	Command	Description
Enter system view	**system-view**	-
Create a local port mirroring group	**mirroring-group** *group-id* **local**	Required
Configure the destination port	**mirroring-group** *group-id* **monitor-port** *monitor-port*	Required LACP must be disabled on the mirroring destination port and you are recommended to disable STP on the mirroring destination port.
Configure the source port and specify the direction of the packets to be mirrored	**mirroring-group** *group-id* **mirroring-port** *mirroring-port-list* { **both** | **inbound** | **outbound** }	Required
Display parameter settings of the local mirroring	**display mirroring-group** { **all** | **local** }	Optional This command can be executed in any view.

Configuration Example

- The source port is GigabitEthernet 2/0/1. Mirror all packets received and sent via this port.
- The destination port is GigabitEthernet 2/0/4.

1 Configuration procedure 1:

```
<SW7750> system-view
[SW7750] mirroring-group 1 local
[SW7750] interface GigabitEthernet 2/0/4
[SW7750-GigabitEthernet2/0/4] mirroring-group 1 monitor-port
```

```
[SW7750-GigabitEthernet2/0/4] quit
[SW7750] interface GigabitEthernet 2/0/1
[SW7750-GigabitEthernet2/0/1] mirroring-group 1 mirroring-port both
```

2 Configuration procedure 2:

```
<SW7750> system-view
[SW7750] mirroring-group 1 local
[SW7750] mirroring-group 1 monitor-port GigabitEthernet 2/0/4
[SW7750] mirroring-group 1 mirroring-port GigabitEthernet 2/0/1 both
```

Configuring Remote Port Mirroring

Configuration prerequisites

- The source switch, intermediate switch, and the destination switch have been determined.
- The source port, the reflector port, the destination port, and the remote-probe VLAN have been determined.
- Required configurations are performed to ensure Layer 2 connectivity between the source and destination switches over the remote-probe VLAN.
- The direction of the packets to be monitored has been determined.
- The remote-probe VLAN is enabled.

Configuring remote port mirroring on the source switch

Table 556 Configure remote port mirroring on the source switch

Operation	Command	Description
Enter system view	**system-view**	-
Create a VLAN and enter its VLAN view	**vlan** *vlan-id*	*vlan-id* is the ID of the destination remote-probe VLAN.
Define the current VLAN as a remote-probe VLAN	**remote-probe vlan enable**	Required
Exit current view	**quit**	-
Enter port view of the relay port that connects to the intermediate switch or destination switch	**interface** *interface-type interface-number*	-
Configure the current port as a trunk port	**port link-type trunk**	Required By default, the type of the port is access.
Configure the relay port to permit packets from the remote-probe VLAN to pass	**port trunk permit vlan** *remote-probe-vlan-id*	Required This setting is required for source switch ports that connected with the intermediate switch or destination switch.
Exit current view	**quit**	-
Configure a remote source mirroring group	**mirroring-group** *group-id* **remote-source**	Required
Configure a source port for remote mirroring	**mirroring-group** *group-id* **mirroring-port** *mirroring-port-list* { **both** | **inbound** | **outbound** }	Required

Table 556 Configure remote port mirroring on the source switch

Operation	Command	Description
Configure a remote reflector port	**mirroring-group** *group-id* **reflector-port** *reflector-port*	Required The remote reflector port must be of the Access type. LACP and must be disabled on this port and you are recommended to disable STP on this port. After a port is configured as a reflector port, the switch does not allow you to perform any of the following configurations: ■ Changing the port type and its default VLAN ID ■ Add it to another VLAN
Configure the remote-probe VLAN for the remote source mirroring group	**mirroring-group** *group-id* **remote-probe vlan** *remote-probe-vlan-id*	Required
Display the configuration of the remote source mirroring group	**display mirroring-group remote-source**	Optional This command can be executed in any view.



- *For a centralized I/O Module, if multiple source ports are specified in remote port mirroring configuration, all the source ports must be on the same I/O Module.*
- *You can configure only one reflector port of a remote source mirroring group or one destination port of a local mirroring group on each centralized I/O Module. As for the distributed system, you can configure only one reflector port of a remote source mirroring group or one destination port of a local mirroring group for the whole system. Only one mirroring destination I/O Module can be configured for the centralized or distributed system, and can be referenced by only one local mirroring group.*
- *To mirror tagged packets, you need to configure VLAN VPN on the reflector port.*
- *The reflector ports are mutually exclusive with STP or DLDP. That is, if STP or DLDP is enabled on a port, you are not recommended to configure it as a reflector port; and vice versa, you are not recommended to enable STP or DLDP on a reflector port.*
- *The reflector port cannot forward traffics as a normal port. Therefore, it is recommended that you use an idle and in-down-state port as the reflector port, and be careful to not add other settings on this port.*
- *Be sure not to configure a port used to connect the intermediate and destination switches as the mirroring source port. Otherwise traffic disorder may occur in the network.*

Configuring remote port mirroring on the intermediate switch

Table 557 Configure remote port mirroring on the intermediate switch

Operation	Command	Description
Enter system view	**system-view**	-
Create a remote-probe VLAN and enter VLAN view	**vlan** *vlan-id*	*vlan-id* is the ID of the remote-probe VLAN.
Define the current VLAN as a remote-probe VLAN	**remote-probe vlan enable**	Required
Exit current view	**quit**	-
Enter port view of the relay port through which the intermediate switch is connected to the source switch, destination switch or another intermediate switch	**interface** *interface-type interface-number*	-
Configure the current port as a trunk port	**port link-type trunk**	Required By default, the type of the port is access.
Configure the relay port to permit packets from the remote-probe VLAN to pass	**port trunk permit vlan** *remote-probe-vlan-id*	Required This configuration is necessary for ports on the intermediate switch that are connected to the source switch or the destination switch.

When a switch functions as the intermediate device or destination device for remote mirroring, you are recommended to configure traffic redirect on the incoming port in order to guarantee data mirroring is achieved normally. By configuring traffic redirect, you can redirect all packets of the remote-probe VLAN to the corresponding outgoing port (on the intermediate device) or mirroring destination port (on the destination device). If you want to mirror packets in both directions, you must configure traffic redirect on the incoming port because the incoming port learns the source MAC addresses and destination MAC addresses of packets at the same time. If the incoming port of a packet is the same as the outgoing port of the packet, the packet is dropped. Refer to "Configuring Redirect" on page 673 for configuring traffic redirect.

Configuring remote port mirroring on the destination switch

Table 558 Configure remote port mirroring on the destination switch

Operation	Command	Description
Enter system view	**system-view**	-
Create a remote-probe VLAN and enter VLAN view	**vlan** *vlan-id*	*vlan-id* is the ID of the remote-probe VLAN.
Define the current VLAN as a remote-probe VLAN	**remote-probe vlan enable**	Required
Exit the current view	**quit**	-

Table 558 Configure remote port mirroring on the destination switch

Operation	Command	Description
Enter port view of the relay port through which the destination switch is connected to the source switch or an intermediate switch	**interface** *interface-type interface-number*	-
Configure the current port as a trunk port	**port link-type trunk**	Required By default, the type of the port is access.
Configure the relay port to permit packets from the remote-probe VLAN to pass	**port trunk permit vlan** *remote*-probe-*vlan-id*	Required This configuration is necessary for ports through which the destination switch is connected to the source switch or an intermediate switch.
Exit current view	**quit**	-
Configure the remote destination mirroring group	**mirroring-group** *group-id* **remote-destination**	Required
Configure the destination port for remote mirroring	**mirroring-group** *group-id* **monitor-port** *monitor-port*	Required The destination port for remote mirroring must be of the Access type. LACP must be disabled on this port and you are recommended to disable STP on this port. After you configure a port as the destination port for remote mirroring, the switch does not allow you to change the port type or default VLAN ID of the port.
Configure the remote-probe VLAN for the remote destination mirroring group	**mirroring-group** *group-id* **remote-probe vlan** *remote-probe-vlan-id*	Required
Display the configuration of the remote destination mirroring group	**display mirroring-group remote-destination**	Optional This command can be executed in any view.



- *When a switch functions as the intermediate device or destination device for remote mirroring, you are recommended to configure traffic redirect on the incoming port in order to guarantee data mirroring is achieved normally. By configuring traffic redirect, you can redirect all packets of the remote-probe VLAN to the corresponding outgoing port (on the intermediate device) or mirroring destination port (on the destination device). If you want to mirror packets in both directions, you must configure traffic redirect on the incoming port because the incoming port learns the source MAC addresses and destination MAC addresses of packets at the same time. If the incoming port of a packet is the same as the outgoing port of the packet, the packet is dropped. Refer to "Configuring Redirect" on page 673 for configuring traffic redirect.*
- *You can configure only one reflector port of a remote source mirroring group or one destination port of a local mirroring group on each centralized I/O*

Module. As for the distributed system, you can configure only one reflector port of a remote source mirroring group or one destination port of a local mirroring group for the whole system. Only one mirroring destination I/O Module can be configured for the centralized or distributed system, and can be referenced by only one local mirroring group.

Configuration example

1 Network requirements:

- Switch A is connected to the data detect device via GigabitEthernet 2/0/2.
- GigabitEthernet 2/0/1, the relay port of Switch A, is connected to GigabitEthernet 2/0/1, the relay port of Switch B.
- GigabitEthernet 2/0/2, the relay port of Switch B, is connected to GigabitEthernet 2/0/1, the relay port of Switch C.
- GigabitEthernet 2/0/2, the port of Switch C, is connected to PC1.

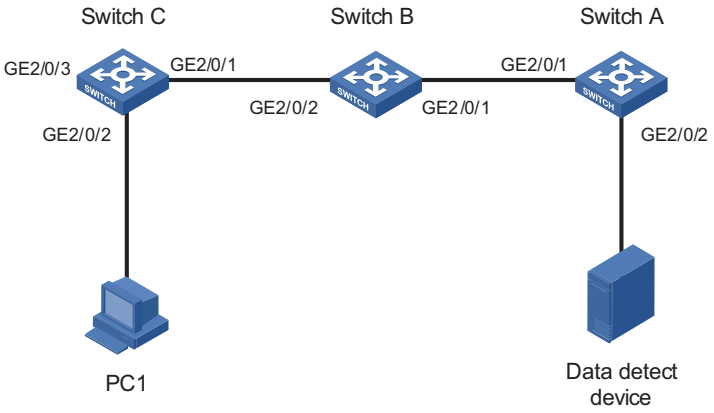
The purpose is to monitor and analyze the packets sent and received by PC1 via the data detect device.

To meet the requirement above by using the remote port mirroring function, perform the following configuration:

- Define VLAN10 as remote-probe VLAN.
- Define Switch A as the destination switch; configure GigabitEthernet 2/0/2, the port that is connected to the data detect device, as the destination port for remote mirroring. Set GigabitEthernet 2/0/2 to an Access port, where LACP must be disabled and STP is recommended to be disabled.
- Define Switch B as the intermediate switch.
- Define Switch C as the source switch, GigabitEthernet 2/0/2 as the source port for remote mirroring, and GigabitEthernet 2/0/3 as the reflector port. Set GigabitEthernet 2/0/3 to an Access port, where LACP must be disabled and STP is recommended to be disabled.

2 Network diagram

Figure 180 Network diagram for remote port mirroring



- Configuration procedure

3 # Configure Switch C.

```
<SW7750> system-view
[SW7750] vlan 10
[SW7750-vlan10] remote-probe vlan enable
[SW7750-vlan10] quit
[SW7750] interface GigabitEthernet 2/0/1
[SW7750-GigabitEthernet2/0/1] port link-type trunk
[SW7750-GigabitEthernet2/0/1] port trunk permit vlan 10
[SW7750-GigabitEthernet2/0/1] quit
[SW7750] mirroring-group 1 remote-source
[SW7750] mirroring-group 1 mirroring-port GigabitEthernet 2/0/2 both
[SW7750] mirroring-group 1 reflector-port GigabitEthernet 2/0/3
[SW7750] mirroring-group 1 remote-probe vlan 10
[SW7750] display mirroring-group remote-source
mirroring-group 1:    type: remote-source    status: active    mirro
ring port:        GigabitEthernet2/0/2  both    reflector port: Giga
bitEthernet2/0/3    remote-probe vlan: 10
```

Configure Switch B.

```
<SW7750> system-view
[SW7750] vlan 10
[SW7750-vlan10] remote-probe vlan enable
[SW7750-vlan10] quit
[SW7750] interface GigabitEthernet 2/0/1
[SW7750-GigabitEthernet2/0/1] port link-type trunk
[SW7750-GigabitEthernet2/0/1] port trunk permit vlan 10
[SW7750-GigabitEthernet2/0/1] quit
[SW7750] interface GigabitEthernet 2/0/2
[SW7750-GigabitEthernet2/0/2] port link-type trunk
[SW7750-GigabitEthernet2/0/2] port trunk permit vlan 10
[SW7750-GigabitEthernet2/0/2] quit
[SW7750] acl number 4500
[SW7750-acl-link-4500] rule 1 permit ingress 10
[SW7750-acl-link-4500] quit
[SW7750] interface GigabitEthernet 2/0/2
[SW7750-GigabitEthernet2/0/2] qos
[SW7750-qosb-GigabitEthernet2/0/2] traffic-redirect inbound link-gro
up 4500 rule 1 interface GigabitEthernet 2/0/1
```

Configure Switch A.

```
<SW7750> system-view
[SW7750] vlan 10
[SW7750-vlan10] remote-probe vlan enable
[SW7750-vlan10] quit
[SW7750] interface GigabitEthernet 2/0/1
[SW7750-GigabitEthernet2/0/1] port link-type trunk
[SW7750-GigabitEthernet2/0/1] port trunk permit vlan 10
[SW7750-GigabitEthernet2/0/1] quit
[SW7750] acl number 4500
[SW7750-acl-link-4500] rule 1 permit ingress 10
[SW7750-acl-link-4500] quit
[SW7750] interface GigabitEthernet 2/0/1
[SW7750-GigabitEthernet2/0/1] qos
[SW7750-qosb-GigabitEthernet2/0/1] traffic-redirect inbound link-gro
up 4500 rule 1 interface GigabitEthernet 2/0/2
[SW7750-qosb-GigabitEthernet2/0/1] quit
[SW7750-GigabitEthernet2/0/1] quit
```

```
[SW7750] mirroring-group 1 remote-destination
[SW7750] mirroring-group 1 monitor-port GigabitEthernet 2/0/2
[SW7750] mirroring-group 1 remote-probe vlan 10
[SW7750] display mirroring-group remote-destination
mirroring-group 1:    type: remote-destination    status: active
monitor port: GigabitEthernet2/0/2    remote-probe vlan: 10
```

Configuring Local Traffic Mirroring

Configuration prerequisites

- ACLs for identifying traffics have been defined. For defining ACLs, see "ACL Configuration" on page 637.
- The destination port has been defined.
- The port on which to perform traffic mirroring configuration and the direction of traffic mirroring has been determined.

Configuration procedure

Table 559 Configure traffic mirroring in Ethernet port view

Operation	Command	Description
Enter system view	**system-view**	-
Create a mirroring group	**mirroring-group** *group-id* **local**	Required
Define the destination port	**mirroring-group** *group-id* **monitor-port** *monitor-port*	Required LACP must be disabled on the mirroring destination port and you are recommended to disable STP on the mirroring destination port.
Enter Ethernet port view of the source port	**interface** *interface-type interface-number*	-
Enter QoS view	**qos**	-
Reference ACLs for identifying traffic flows and perform traffic mirroring for packets that match.	**mirrored-to inbound** *acl-rule* [**system-index** *system-index*] { **interface** *interface-type interface-number* | **mirroring-group** *group-id* }	Required
Display the parameter settings of traffic mirroring	**display qos-interface** [*interface-type interface-number*] **mirrored-to**	Optional These commands can be executed in any view.
Display all QoS settings of a port	**display qos-interface** [*interface-type interface-number*] **all**	

acl-rule: Applied ACL rules, the following table describes the ACL combinations.

Table 560 Combined application of ACLs on I/O Module other than A type.

Combination mode	Form of acl-rule
Apply all rules in an IP type ACL separately	**ip-group** { *acl-number* | *acl-name* }
Apply one rule in an IP type ACL separately	**ip-group** { *acl-number* | *acl-name* } **rule** *rule-id*
Apply all rules in a link type ACL separately	**link-group** { *acl-number* | *acl-name* }

Table 560 Combined application of ACLs on I/O Module other than A type.

Combination mode	Form of acl-rule
Apply one rule in a link type separately	**link-group** { *acl-number* | *acl-name* } **rule** *rule-id*
Apply all rules in a user-defined ACL separately	**user-group** { *acl-number* | *acl-name* }
Apply one rule in a user-defined ACL separately	**user-group** { *acl-number* | *acl-name* } **rule** *rule-id*
Apply one rule in an IP type ACL and one rule in a Link type ACL simultaneously	**ip-group** { *acl-number* | *acl-name* } **rule** *rule-id* **link-group** { *acl-number* | *acl-name* } **rule** *rule-id*

- *Only non-type-A I/O Modules support the traffic mirroring configuration.*
- *To define a destination port for mirroring, you can also enter the port view of the specified port directly to execute the* ***mirroring-group*** *group-id* ***monitor-port*** *command. Refer to corresponding command manual for detail.*

Configuration example

1 Network requirements:

- GigabitEthernet 2/0/1 on the switch is connected to the 10.1.1.1/24 network segment.
- Mirror the packets from the 10.1.1.1/24 network segment to GigabitEthernet 2/0/4, the destination port.

2 Configuration procedure:

```
<SW7750> system-view
[SW7750] acl number 2000
[SW7750-acl-basic-2000] rule permit source 10.1.1.1 0.0.0.255
[SW7750-acl-basic-2000] quit
[SW7750] mirroring-group 3 local
[SW7750] mirroring-group 3 monitor-port GigabitEthernet 2/0/4
[SW7750] interface GigabitEthernet 2/0/1
[SW7750-GigabitEthernet2/0/1] qos
[SW7750-qosb-GigabitEthernet2/0/1] mirrored-to inbound ip-group 2000
 interface GigabitEthernet 2/0/4
```

Configuring Remote Traffic Mirroring

Configuration prerequisites

- ACLs for identifying traffics have been defined. For defining ACLs, refer to "ACL Configuration" on page 637.
- The source switch, intermediate switch and the destination switch have been specified.
- The reflector port, destination port for mirroring, and remote-probe VLAN have been specified.
- Required configurations are performed to ensure Layer 2 connectivity between the source and destination switches over the remote-probe VLAN.
- The direction of traffic packets to be monitored has been determined.
- The remote-probe VLAN has been enabled.

Configuring the source switch

Table 561 Configure the source switch

Operation	Command	Description
Enter system view	**system-view**	-
Create a VLAN and enter the VLAN view	**vlan** *vlan-id*	The *vlan-id* is the ID of the remote-probe VLAN to be defined.
Define the current VLAN as the remote-probe VLAN	**remote-probe vlan enable**	Required
Quit from the current view	**quit**	-
Enter port view of the relay port connected with an intermediate switch or a destination switch	**interface** *interface-type interface-number*	-
Configure the current port as a trunk port	**port link-type trunk**	Required By default, the type of the port is access.
Configure the relay port to permit packets from the remote-probe VLAN to pass.	**port trunk permit vlan** *remote-probe-vlan-id*	Required This configuration is required on the source switch ports that connect with the intermediate switch and the destination switch must be configured so.
Quit from the current view	**quit**	-
Configure the remote source mirroring group	**mirroring-group** *group-id* **remote-source**	Required
Configure the remote reflector port	**mirroring-group** *group-id* **reflector-port** *reflector-port*	Required The remote reflector port must be Access port, where LACP must be disabled and STP is recommended to be disabled. After a port is configured as reflector port, you can neither change the port type and the default VLAN ID nor add the reflector port to other VLANs.
Configure the remote-probe VLAN of the remote source mirroring group	**mirroring-group** *group-id* **remote-probe vlan** *remote-probe-vlan-id*	Required
Ether Ethernet port view of the source port	**interface** *interface-type interface-number*	-
Enter QoS view	**qos**	-
Reference ACLs for identifying traffic flows and perform traffic mirroring for packets that match.	**mirrored-to inbound** *acl-rule* [**system-index** *system-index*] { **interface** *interface-type interface-number* **reflector** | **mirroring-group** *group-id* }	Required

Table 561 Configure the source switch

Operation	Command	Description
Display configuration of the remote source mirroring group	**display mirroring-group remote-source**	Optional You can execute the **display** command in any view.
Display the parameter settings of traffic mirroring	**display qos-interface** [*interface-type interface-number*] **mirrored-to**	
Display all QoS settings of a port	**display qos-interface** [*interface-type interface-number*] **all**	

acl-rule: Applied ACL rules, for the ACL combinations of service modules other than A type, refer to Table 560.



- *Only non-type-A I/O Modules support the traffic mirroring configuration.*
- *You can configure only one reflector port of a remote source mirroring group or one destination port of a local mirroring group on each centralized I/O Module. As for the distributed system, you can configure only one reflector port of a remote source mirroring group or one destination port of a local mirroring group for the whole system. Only one mirroring destination I/O Module can be configured for the centralized or distributed system, and can be referenced by only one local mirroring group.*
- *If you want to mirror the tagged packets, you need to configure VLAN VPN on the reflector port.*
- *For the reflector port can not forward traffic as a normal port does, you are recommended to configure the port that is not in use to be the reflector port and not to perform other configurations on this port.*

Configuring the intermediate switch

Configuring an intermediate switch is the same as configuring remote port mirroring on the intermediate switch. Refer to "Configuring remote port mirroring on the intermediate switch" on page 692 for details.

Configuring the destination switch

Configuring a destination switch is the same as configuring remote port mirroring on the destination switch. Refer to "Configuring remote port mirroring on the destination switch" on page 692."

Configuration example

1 Network requirements:

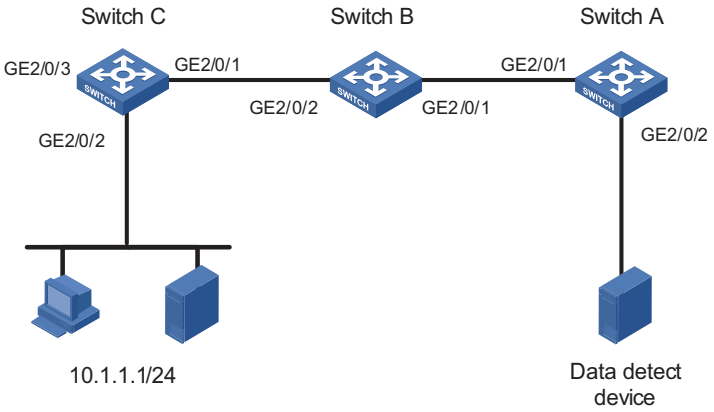
- Switch A is connected to the data detect device through GigabitEthernet 2/0/2.
- GigabitEthernet 2/0/1, the relay port of Switch A, is connected to GigabitEthernet 2/0/1, the relay port of Switch B.
- GigabitEthernet 2/0/2, the relay port of Switch B, is connected to GigabitEthernet 2/0/1, the relay port of Switch C.
- GigabitEthernet 2/0/2, the port of Switch C, is connected to the 10.1.1.1/24 network segment.

Use the remote traffic mirroring function to mirror the packets from the 10.1.1.1/24 network segment to GigabitEthernet 2/0/2, the port of Switch A, so that the data detect device can monitor the traffic:

- Define VLAN10 as remote-probe VLAN.
- Define Switch A as the destination switch; configure GigabitEthernet 2/0/2, the port that is connected to the data detect device, as the destination port for remote mirroring. Set GigabitEthernet2/0/2 to an Access port, where LACP must be disabled and STP is recommended to be disabled.
- Define Switch B as the intermediate switch.
- Define Switch C as the source switch, GigabitEthernet 2/0/3 as the reflector port. Set GigabitEthernet 2/0/3 to an Access port, with STP and LACP disabled. Configure the traffic mirroring function on GigabitEthernet 2/0/2.

2 Network diagram

Figure 181 Network diagram for remote traffic mirroring



3 Configuration procedure

Configure Switch A.

```
<SW7750> system-view
[SW7750] vlan 10
[SW7750-vlan10] remote-probe vlan enable
[SW7750-vlan10] quit
[SW7750] interface GigabitEthernet 2/0/1
[SW7750-GigabitEthernet2/0/1] port link-type trunk
[SW7750-GigabitEthernet2/0/1] port trunk permit vlan 10
[SW7750-GigabitEthernet2/0/1] quit
[SW7750] mirroring-group 1 remote-destination
[SW7750] mirroring-group 1 monitor-port GigabitEthernet 2/0/2
[SW7750] mirroring-group 1 remote-probe vlan 10
[SW7750] display mirroring-group remote-destination
mirroring-group 1:    type: remote-destination    status: active
monitor port: GigabitEthernet2/0/2    remote-probe vlan: 10
```

Configure Switch B

```
<SW7750> system-view
[SW7750] vlan 10
[SW7750-vlan10] remote-probe vlan enable
```

```
[SW7750-vlan10] quit
[SW7750] interface GigabitEthernet 2/0/1
[SW7750-GigabitEthernet2/0/1] port link-type trunk
[SW7750-GigabitEthernet2/0/1] port trunk permit vlan 10
[SW7750-GigabitEthernet2/0/1] quit
[SW7750] interface GigabitEthernet 2/0/2
[SW7750-GigabitEthernet2/0/1] port link-type trunk
[SW7750-GigabitEthernet2/0/2] port trunk permit vlan 10
```

Configure Switch C

```
<SW7750> system-view
[SW7750] acl number 2000
[SW7750-acl-basic-2000] rule permit source 10.1.1.1 0.0.0.255
[SW7750-acl-basic-2000] quit
[SW7750] vlan 10
[SW7750-vlan10] remote-probe vlan enable
[SW7750-vlan10] quit
[SW7750] interface GigabitEthernet 2/0/1
[SW7750-GigabitEthernet2/0/1] port link-type trunk
[SW7750-GigabitEthernet2/0/1] port trunk permit vlan 10
[SW7750-GigabitEthernet2/0/1] quit
[SW7750] mirroring-group 1 remote-source
[SW7750] mirroring-group 1 reflector-port GigabitEthernet 2/0/3
[SW7750] mirroring-group 1 remote-probe vlan 10
[SW7750] interface GigabitEthernet 2/0/2
[SW7750-GigabitEthernet2/0/2] qos
[SW7750-qosb-GigabitEthernet2/0/2] mirrored-to inbound ip-group 2000
 interface GigabitEthernet 2/0/3 reflector
[SW7750-qosb-GigabitEthernet2/0/2] display qos-interface GigabitEthe
rnet2/0/2 mirrored-to

GigabitEthernet2/0/2: mirrored-to
 Inbound:
   Matches: Acl 2000 rule 0  running
     Mirrored to: mirroring-group 1
```

Configuring Mirroring to Local I/O Module

Configuration prerequisites

- The mirroring source port or the mirroring source I/O Module is specified, that is, the direction of mirrored packets is specified.
- The mirroring destination I/O Module is specified.

Configuration procedure

Table 562 Configure mirroring to LS81VSNP

Operation	Command	Description
Enter system view	**system-view**	-
Create port mirroring groups	**mirroring-group** *group-id* **local**	Required
Define the mirroring destination I/O Module	**mirroring-group** *group-id* **monitor-slot** *slot-number*	Required The mirroring destination I/O Module must be LS81VSNP or LS82VSNP.

Table 562 Configure mirroring to LS81VSNP

Operation	Command	Description
Define the mirroring source port or mirroring source I/O Module	**mirroring-group** *group-id* **mirroring-port** *mirroring-port-list* { **both** | **inbound** | **outbound** }	You must perform one of the two operations. The mirroring source I/O Module can be a distributed or centralized I/O Module; however, the mirroring source ports must be ports on distributed I/O Modules. Mirroring source ports can also be configured in Ethernet port view. For detailed information, refer to "Configuring port mirroring in Ethernet port view" on page 688."
	mirroring-group *group-id* **mirroring-slot** *slot-number* { **inbound** | **outbound** | **both** }	
Display the settings about mirroring	**display mirroring-group** { **all** | **local** }	Optional You can execute the **display** command in any view.

Configuration example

- The mirroring source I/O Module resides in slot 3 and all the packets sent or received on the I/O Module are mirrored.
- The mirroring destination I/O Module resides in slot 4.

Configuration procedure:

```
<SW7750> system-view
[SW7750] mirroring-group 1 local
[SW7750] mirroring-group 1 monitor-slot 4
[SW7750] mirroring-group 1 mirroring-slot 3 both
```

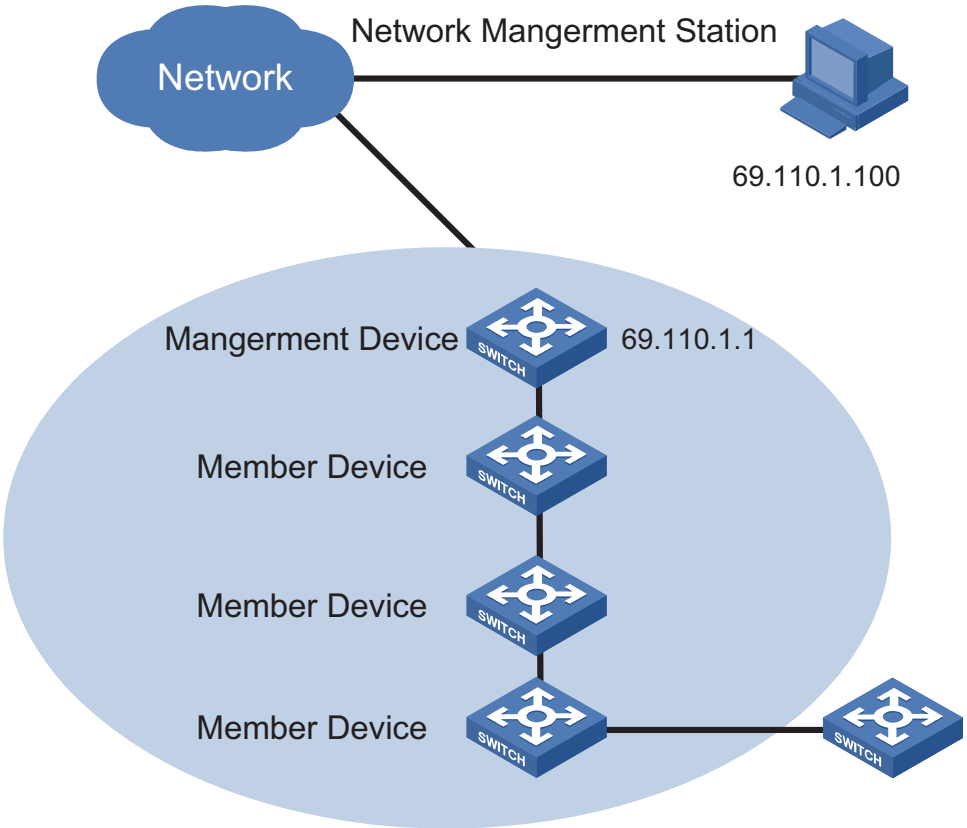
63 CLUSTER

Cluster Overview

Introduction to Switch Clustering V2

A cluster is implemented through Switch Clustering V2. By employing the group management protocol (Switch Clustering V2), a network administrator can manage multiple switches using the public IP address of a switch known as a management device. The switches under the management of the management device are member devices. The management device, along with the member devices, forms a cluster. Normally, a cluster member device is not assigned a public IP address. Management and maintenance operations intended for the member devices in a cluster are redirected by the management device. Figure 182illustrates a typical cluster implementation.

Figure 182 Diagram for cluster



Switch Clustering V2 offers the following advantages:

- The procedures to configure multiple switches remarkably simplified. When the management device is assigned a public IP address, you can configure/manage

a specific member device on the management device instead of logging into it in advance.

- Functions of topology discovery and display provided, which assist network monitoring and debugging
- Software upgrading and parameter configuring can be performed simultaneously on multiple switches.
- Free of topology and distance limitations
- Saving IP address resource

Switch Clustering V2 is comprised of the following three protocols:

- Neighbor discovery protocol (NDP): Switch Clustering V2 implements NDP to discover the information about the directly connected neighbor devices, including device type, software/hardware version, connecting port and so on. The information such as device ID, port mode (duplex or half duplex), product version, and BootROM version can also be given.
- Neighbor topology discovery protocol (NTDP): Switch Clustering V2 implements NTDP to collect the information about the network topology, including the device connections and the device information in the network. The hop range for topology discovery can be adjusted manually.
- Cluster management protocol: The cluster management protocol provides the member recognition and member management function. It can also perform large-scaled device management together with the network administrator. Member recognition means that the management device recognizes each member in the cluster through locating each member and then distributes the configuration and management commands to members. Member management means to manage the following events through the management device, including adding a member, removing a member, and the member's authentication on the management device. Member management also manages the cluster parameters including interval of sending handshake packets, management VLAN of the cluster, public FTP server of the cluster.

Cluster-related configurations are described in the following sections.

Introduction to NDP

NDP is the protocol for discovering the information about the adjacent nodes. NDP operates on the data link layer, so it supports different network layer protocols.

NDP is used to discover the information about directly connected neighbors, including the device type, software/hardware version, and connecting port of the adjacent devices. It can also provide the information concerning device ID, port simplex/duplex status, product version, BootROM version and so on.

An NDP-enabled device maintains an NDP information table. Each entry in an NDP table ages with time. You can also clear the current NDP information manually to have adjacent information collected again.

An NDP-enabled device broadcasts NDP packets regularly to all ports in up state. An NDP packet carries the holdtime field, which indicates the period for the receiving devices to keep the NDP data. Receiving devices only store the information carried in the received NDP packets rather than forward them. The corresponding data entry in the NDP table is updated when the received

information is different from the existing one. Otherwise, only the holdtime of the corresponding entry is updated.

Introduction to NTDP

NTDP is a protocol for network topology information collection. NTDP provides the information about the devices that can be added to clusters and collects the topology information within the specified hops for cluster management.

Based on the NDP information table created by NDP, NTDP transmits and forwards NTDP topology collection request to collect the NDP information and neighboring connection information of each device in a specific network range for the management device or the network administrator to implement needed functions.

Upon detecting a change occurred on a neighbor, a member device informs the management device of the change through handshake packets. The management device then collects the specified topology information through NTDP. Such a mechanism enables topology changes to be tracked in time.



As for NTDP implementing, you need to perform configurations on the management device, the member devices, and the candidate devices as follows

- *On the management device, enable NTDP both globally and for specific ports, and configure the NTDP settings.*
- *On each member device and candidate device, enable NTDP both globally and for specific ports. As member devices and candidate devices adopt the NTDP settings configured for the management device, NTDP setting configurations are not needed.*
- *NTDP takes effect in the management VLAN only. Switch 7750 Ethernet switches take VLAN 1 as the management VLAN, that is, the NTDP function of the Switch 7750 takes effect in VLAN 1 only.*

Introduction to Cluster

Introduction to cluster configuration

A cluster has one (and only one) management device. Note the following when creating a cluster:

- You need to designate the management device first. The management device of a cluster is the portal of the cluster. That is, any operations performed in external networks and intended for the member devices of a cluster, such as accessing, configuring, managing, and monitoring, can only be implemented through the management device.
- The management device of a cluster recognizes and controls all the member devices in the cluster, no matter where they are located on the network or how they are connected.
- The management device collects topology information about all the member and candidate devices to provide useful information for users to establish a cluster.
- A management device manages and monitors the devices in the cluster by collecting and processing NDP/NTDP packets. NDP/NTDP packets contain network topology information.

All the above-mentioned operations need the support of the cluster function.

You need to enable the cluster function and configure cluster parameters on a management device. However, you only need to enable the cluster function on the member devices and candidate devices.

Introduction to function of cluster

Cluster provides the function of batch management for the switches in the network. Cluster provides external management and maintenance applications, including SNMP, command line, program and data loading, log report and alarm report. These applications can be divided into internal-to-external applications and external-to-internal applications. All the applications are processed according to the following procedure:

- The communication between the management device and member device in the cluster is implemented through packet interaction in the management VLAN.
- The communication between the cluster and the external server is implemented by the Layer 3 interface of the cluster management VLAN.
- When the member device in the cluster communicates with the external server, the member device transmits the data to the management device first, and then the management device transmits the data to the external server. When the management program running on the external server manages the member device, the external server transmits the protocol packets to the management device first, and then the management device forwards the protocol packets to the member device.

You can configure public FTP servers, TFTP servers, logging hosts and SNMP hosts for the whole cluster. The management device in the cluster is the default public FTP server of the cluster when the public FTP server of the cluster is not configured. Cluster, together with the network management system, can perform large-scaled device management.

The Switch 7750 manage the cluster with VLAN 1 being the management VLAN in the cluster. You are required to configure the IP address of the Layer 3 virtual interface of the management VLAN before setting up a cluster. Otherwise, the cluster cannot be set up successfully. After the cluster is set up, you are not allowed to modify the IP address of the management VLAN interface.

Switch Roles in the Cluster

According to their functions and status in a cluster, switches in the cluster play different roles. You can specify the role a switch plays. A switch also changes its role according to specific rules.

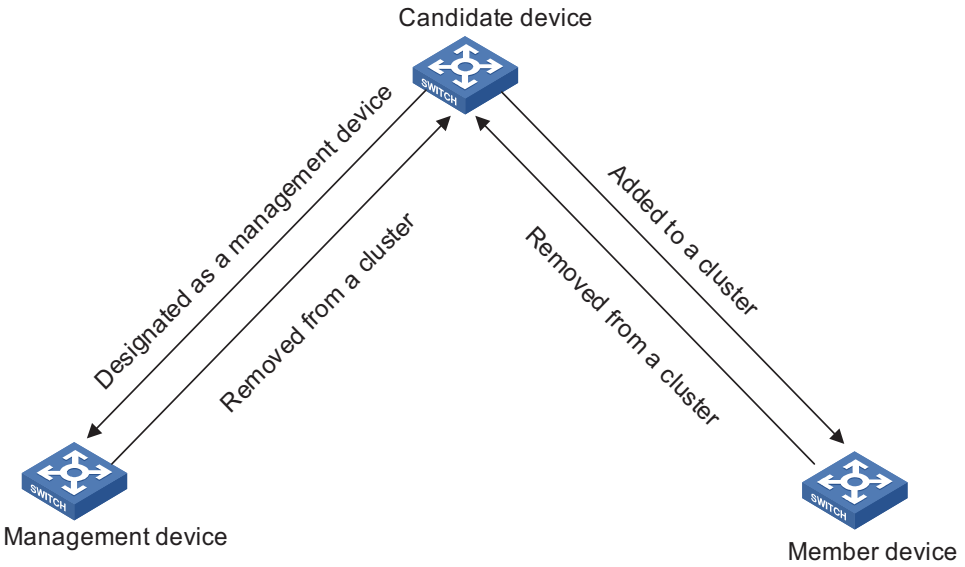
The following three switch roles exist in a cluster: management device, member device, and candidate device.

Table 563 Switch roles in the cluster

Role	Configuration	Description
Management device	■ Configured with a public IP address. ■ Receive management commands that a user sends through the public network and process the received commands	■ Provide management interfaces for all switches in the cluster ■ Manage member devices by redirecting commands, that is, forward the commands to the intended member devices for processing ■ Provide the following functions, including neighbor discovery, topology information collection, cluster management, and cluster state maintenance, and support all types of FTP servers and SNMP host proxies
Member device	Normally, a member device is not configured with a public IP address	■ Member in the cluster ■ Neighbor discovery, being managed by the management device, running commands forwarded by proxies, and failure/log reporting
Candidate device	Normally, a candidate device is not configured with a public IP address	A candidate device is a switch that does not belong to any cluster, although it can be added to a cluster

The switch roles are switched according to the following rules:

Figure 183 Role switching roles



- Each cluster has one (and only one) management device. A management device collects NDP/NTDP information to discover and determine candidate devices, which can be then added into the cluster through manual configurations.
- A candidate device becomes a member device after being added to a cluster.

- A member device becomes a candidate device after being removed from the cluster.

Management Device Configuration

Management Device Configuration Tasks

Table 564 Management device configuration tasks

Operation	Description	Related section
Enable NDP globally and for specific ports	Required	"Enabling NDP Globally and for Specific Ports" on page 708
Configure NDP-related parameters	Optional	"Configuring NDP-related Parameters" on page 708
Enable NTDP globally and for specific ports	Required	"Enabling NTDP Globally and for Specific Ports" on page 709
Configure NTDP-related parameters	Optional	"Configuring NTDP-related Parameters" on page 709
Enable the cluster function	Required	"Enabling the Cluster Function" on page 709
Configure cluster parameters	Required	"Configuring Cluster Parameters" on page 709
Configure interaction for the cluster	Required	"Configuring Interaction for the Cluster" on page 711

Enabling NDP Globally and for Specific Ports

Table 565 Enable NDP globally and for a specific port

Operation			Command	Description
Enter system view			**system-view**	-
Enable NDP globally			**ndp enable**	Required By default, NDP is enabled globally
Enable NDP for the specified Ethernet ports	In system view		**ndp enable interface** *port-list*	You must choose one of them By default, NDP is enabled on the port
	In Ethernet port view	Enter Ethernet port view	**interface** *interface-type interface-number*	
		Enable NDP on the port	**ndp enable**	

Configuring NDP-related Parameters

Table 566 Configure NDP-related parameters

Operation	Command	Description
Enter system view	**system-view**	-
Configure the holdtime of NDP information	**ndp timer aging** *aging-in-seconds*	Optional By default, the aging time of NDP packets is 180 seconds
Configure the interval to send NDP packets	**ndp timer hello** *seconds*	Optional By default, the interval of sending NDP packets is 60 seconds

Enabling NTDP Globally and for Specific Ports

Table 567 Enable NTDP globally and for specific ports

Operation	Command	Description
Enter system view	**system-view**	-
Enable NTDP globally	**ntdp enable**	Required By default, the NTDP is enabled globally.
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Enable NTDP for the Ethernet port	**ntdp enable**	Required By default, the NTDP is enabled for the Ethernet port.

Configuring NTDP-related Parameters

Table 568 Configure NTDP parameters

Operation	Command	Description
Enter system view	**system-view**	-
Configure the range topology information within which is to be collected	**ntdp hop** *hop-value*	Optional By default, the hop range for topology collection is 3 hops
Configure the hop delay to forward topology-collection request packets	**ntdp timer hop-delay** *time*	Optional By default, the delay of the device is 200 ms
Configure the port delay to forward topology collection request packets	**ntdp timer port-delay** *time*	Optional By default, the port delay is 20 ms
Configure the interval to collect topology information	**ntdp timer** *interval-in-minutes*	Optional By default, the interval of topology collection is 0.
Quit system view.	**quit**	-
Start topology information collection	**ntdp explore**	Optional You can use this command to manually start the topology information collection to get the latest topology information.

Enabling the Cluster Function

Table 569 Enable the cluster function

Operation	Command	Description
Enter system view	**system-view**	-
Enable the cluster function globally	**cluster enable**	Optional By default, the cluster function is enabled

Configuring Cluster Parameters



CAUTION: *When configuring a cluster, you must ensure that the routing table is not full. Otherwise, the private IP routes of the cluster cannot be advertised, and*

as a result cluster handshake messages cannot be properly sent or received and devices will repeatedly join or leave the cluster.

- *If the routing table of the administrative device is full upon establishment of a cluster, all candidate devices will repeatedly join or leave the cluster.*
- *If the routing table of the administrative device is full when a candidate device of a cluster joins the cluster, this device will repeatedly join or leave the cluster.*

Creating a cluster and configuring cluster parameters manually

Table 570 Configure cluster parameters manually

Operation	Command	Description
Enter system view	**system-view**	-
Enter VLAN interface view	**interface Vlan-interface** *vlan-id*	Required The Switch 7750 requires you to configure the IP address of the Layer 3 virtual interface of VLAN1 before you set up a cluster. Otherwise, the cluster cannot be set up.
Configure the IP address of the VLAN interface	**ip address** *ip-address* { *mask* | *mask-length* }	Required
Enter cluster view	**cluster**	-
Configure an IP address pool for the cluster	**ip-pool** *administrator-ip-address* { *ip-mask* | *ip-mask-length* }	Required
Build a cluster	**build** *name*	Required The *name* argument specifies the name to be assigned to the cluster. If a cluster is already established, you can use this command to change the name of the cluster.
Configure a multicast MAC address for the cluster	**cluster-mac** *H-H-H*	Required By default, the cluster multicast MAC address is 0180-C200-000A.
Set the interval for the management device to send multicast packets	**cluster-mac syn-interval** *time-interval*	Optional By default, the interval to send multicast packets is one minutes.
Configure the holdtime for a switch	**holdtime** *seconds*	Optional By default, the holdtime is 60 seconds
Set the interval to send handshake packets	**timer** *interval*	Optional By default, the interval to send handshake packets is 10 seconds
Quit cluster view	**quit**	-



For Switch 7750 Ethernet switches, VLAN1 serves as the cluster management VLAN and the IP address of the Layer-3 virtual interface of the management VLAN must be configured before a cluster is created. After the cluster is created, it is prohibited to change the interface IP address of the management VLAN.

Building a cluster automatically

Table 571 Enable the cluster function automatically

Operation	Command	Description
Enter system view	**system-view**	-
Enter VLAN interface view	**interface Vlan-interface** *vlan-id*	Required The Switch 7750 requires you to configure the IP address of the Layer 3 virtual interface of VLAN1 before you set up a cluster. Otherwise, the cluster cannot be set up.
Configure the IP address of the VLAN interface	**ip address** *ip-address* { *mask* | *mask-length* }	Required
Enter cluster view	**cluster**	-
Configure the rang e of the IP addresses of the cluster	**ip-pool** *administrator-ip-address* { *ip-mas k* | *ip-mask-length* }	Required
Build a cluster automatically	**auto-build** [**recover**]	Optional You can build clusters according to corresponding prompts

Configuring Interaction for the Cluster

Table 572 Configure interaction for the cluster

Operation	Command	Description
Enter system view	**system-view**	-
Enter cluster view	**cluster**	Required
Configure the public FTP server for the cluster	**ftp-server** *ip-address*	Optional
Configure the TFTP server for the cluster	**tftp-server** *ip-address*	Optional
Configure the logging host for the cluster	**logging-host** *ip-address*	Optional
Configure the SNMP host for the cluster	**snmp-host** *ip-address*	Optional

CAUTION: *For Switch 7750 Ethernet switches, the IP address of the cluster public FTP/TFTP server must be in the same network segment as that of the Layer-3 interface of management VLAN (VLAN1). Otherwise, member devices cannot communicate with the cluster public FTP/TFTP server.*

Member Device Configuration

Member Device Configuration Tasks

Table 573 Member device configuration tasks

Operation	Description	Related section
Enable NDP globally and for specific ports	Required	"Enabling NDP Globally and for Specific Ports" on page 712
Enable NTDP globally and for specific ports	Required	"Enabling NTDP Globally and for Specific Ports" on page 712

Table 573 Member device configuration tasks

Operation	Description	Related section
Configure member devices to access FTP/TFTP server of the cluster	Optional	"Configure Member Devices to Access FTP/TFTP Server of the Cluster" on page 712

Enabling NDP Globally and for Specific Ports

Table 574 Enable NDP globally and for specific ports

Operation			Command	Description
Enter system view			**system-view**	-
Enable NDP globally			**ndp enable**	Required By default, the NDP is enabled globally.
Enable NDP for specified ports	In system view		**ndp enable interface** *port-list*	Required By default, the NDP is enabled for the port. You can choose to enable NDP in system view or in Ethernet port view
	In Ethernet port view	Enter Ethernet port view	**interface** *interface-type interface-number*	
		Enable NDP on the port	**ndp enable**	

Enabling NTDP Globally and for Specific Ports

Table 575 Enable NTDP globally and for specific ports

Operation	Command	Description
Enter system view	**system-view**	-
Enable system NTDP	**ntdp enable**	Required By default, the NTDP is enabled globally.
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Enable NTDP for the port	**ntdp enable**	Required By default, the NTDP is enabled for the port.

Configure Member Devices to Access FTP/TFTP Server of the Cluster

Perform the following configuration in user view of the member device.

Table 576 Configure member devices to access FTP/TFTP server of the cluster

Operation	Command	Description
Access the public FTP server of the cluster	**ftp cluster**	Optional
Download files from the public TFTP server of the cluster	**tftp cluster get** *source-file* [*destination-file*]	Optional
Upload files to the public TFTP server of the cluster	**tftp cluster put** *source-file* [*destination-file*]	Optional

Intra-Cluster Configuration

Table 577 Configure a cluster

Operation	Command	Description
Enter system view	**system-view**	-
Enter cluster view	**cluster**	-
Add a candidate device to a cluster	**add-member** [*member-number*] **mac-address** *H-H-H* [**password** *password*]	Optional
Remove a member device from the cluster	**delete-member** *member-num*	Optional
Reboot a specified member device	**reboot member** { *member-num* | **mac-address** *H-H-H* } [**eraseflash**]	Optional
Return to system view	**quit**	-
Return to user view	**quit**	-
Switch between the management device view and a member device view	**cluster switch-to** { *member-number* | **mac-address** *H-H-H* | **administrator** }	Optional Switch between the management device view and the member device view

*After a cluster is established, SNMP Trap is enabled when Switch 7750s join the cluster as candidate devices or leave the cluster as member devices. You can use the **undo snmp trap enable** command to disable SNMP Trap.*

Displaying and Maintaining a Cluster

After the configuration above, you can execute the **display** command to display the running status after the cluster configuration. You can verify the configuration effect through checking the displayed information.

Table 578 Display and maintain cluster configurations

Operation	Command	Description
Display the global NDP configuration (including the interval to send NDP packets and the holdtime)	**display ndp**	Optional You can execute the **display** command in any view
Display the information about the neighbors discovered by NDP and connected to specified ports	**display ndp interface** *port-list*	
Display the global NTDP information	**display ntdp**	
Display device information collected through NTDP	**display ntdp device-list** [**verbose**]	
Display state and statistics information about a cluster	**display cluster**	
Display the information about the candidate devices of a cluster	**display cluster candidates** [**mac-address** *H-H-H* | **verbose**]	
Display the information about the cluster members	**display cluster members** [*member-num* | **verbose**]	

Table 578 Display and maintain cluster configurations

Operation	Command	Description
Clear the NDP statistics on a port	**reset ndp statistics** [**interface** *port-list*]	-

Cluster Configuration Example

Cluster Configuration Example

Network requirements

Three switches form a cluster, in which:

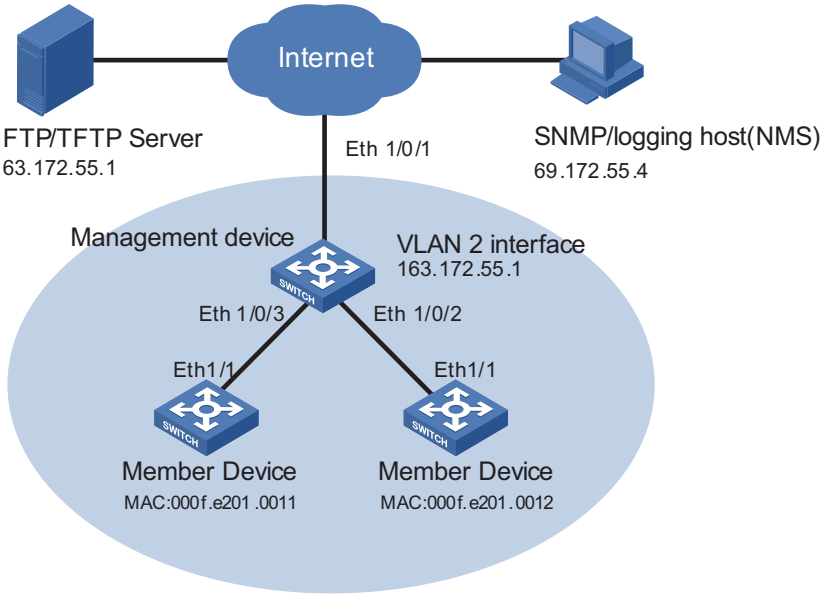
- The management device is a Switch 7750.
- The rest are member devices.

The Switch 7750 manages the rest two member devices as the management device. The detailed information about the cluster is as follows.

- The two member devices are connected to Ethernet1/0/2 and Ethernet1/0/3 ports of the management device.
- The management device is connected to the external network through its Ethernet1/0/1 port.
- Ethernet1/0/1 port of the management device belongs to VLAN1, whose interface IP address is 163.172.55.1.
- All the devices in the cluster use the same FTP server and TFTP server.
- The FTP server and TFTP server share one IP address: 163.172.55.2.
- The SNMP site and log host share one IP address: 69.172.55.4.

Network diagram

Figure 184 Network diagram for Switch Clustering cluster configuration



Configuration procedure

1 Configure the member devices (taking one member as an example)

Enable NDP globally and for Ethernet1/1.

```
<SW7750> system-view
[SW7750] ndp enable
[SW7750] interface Ethernet 1/1
[SW7750-Ethernet1/1] ndp enable
[SW7750-Ethernet1/1] quit
```

Enable NTDP globally and for Ethernet1/1.

```
[SW7750] ntdp enable
[SW7750] interface Ethernet 1/1
[SW7750-Ethernet1/1] ntdp enable
[SW7750-Ethernet1/1] quit
```

Enable the cluster function.

```
[SW7750] cluster enable
```

2 Configure the management device

Configure the IP address of the management VLAN (the Switch 7750 take VLAN 1 as the default VLAN).

```
<SW7750> system-view
[SW7750] interface Vlan-interface 1
[SW7750-Vlan-interface1] ip address 163.172.55.1
[SW7750-Vlan-interface1] quit
```

Enable NDP globally and on Ethernet1/0/2 and Ethernet1/0/3.

```
[SW7750] ndp enable
[SW7750] interface Ethernet 1/0/2
[SW7750-Ethernet1/0/2] ndp enable
[SW7750-Ethernet1/0/2] interface Ethernet 1/0/3
[SW7750-Ethernet1/0/3] ndp enable
[SW7750-Ethernet1/0/3] quit
```

Configure the holdtime of NDP information to be 200 seconds.

```
[SW7750] ndp timer aging 200
```

Configure the interval to send NDP packets to be 70 seconds.

```
[SW7750] ndp timer hello 70
```

Enable NTDP globally and for Ethernet1/0/2 and Ethernet1/0/3 ports.

```
[SW7750] ntdp enable
[SW7750] interface Ethernet 1/0/2
[SW7750-Ethernet1/0/2] ntdp enable
[SW7750-Ethernet1/0/2] interface Ethernet 1/0/3
[SW7750-Ethernet1/0/3] ntdp enable
[SW7750-Ethernet1/0/3] quit
```

Configure the hop count to collect topology to be 2.

```
[SW7750] ntdp hop 2
```

Configure the delay time for topology-collection request packets to be forwarded on member devices to be 150 ms.

```
[SW7750] ntdp timer hop-delay 150
```

Configure the delay time for topology-collection request packets to be forwarded through the ports of member devices to be 15 ms.

```
[SW7750] ntdp timer port-delay 15
```

Configure the interval to collect topology information to be 3 minutes.

```
[SW7750] ntdp timer 3
```

Enable the cluster function.

```
[SW7750] cluster enable
```

Enter cluster view.

```
[SW7750] cluster
[SW7750-cluster]
```

Configure an IP address pool for the cluster. The IP address in the IP address pool starts from 172.16.0.1. The mask is 255.255.255.248.

```
[SW7750-cluster] ip-pool 172.16.0.1 255.255.255.248
```

Specify a name for the cluster and create the cluster.

```
[SW7750-cluster] build aaa
[aaa_0.3Com-cluster]
```

Add the attached two switches to the cluster.

```
[aaa_0.3Com-cluster] add-member 1 mac-address 00e0-fc01-0011
[aaa_0.3Com-cluster] add-member 17 mac-address 00e0-fc01-0012
```

Configure the holdtime of the member device information to be 100 seconds.

```
[aaa_0.3Com-cluster] holdtime 100
```

Configure the interval to send handshake packets to be 10 seconds.

```
[aaa_0.3Com-cluster] timer 10
```

Configure the FTP Server, TFTP Server, Log host and SNMP host for the cluster.

```
[aaa_0.3Com-cluster] ftp-server 163.172.55.2
[aaa_0.3Com-cluster] tftp-server 163.172.55.2
[aaa_0.3Com-cluster] logging-host 69.172.55.4
[aaa_0.3Com-cluster] snmp-host 69.172.55.4
```

3 Configure the member devices (taking one member as an example)

Add the devices connected to the management device into the cluster and perform the following configuration on the member device.

Connect the member device to the public remote FTP server of the cluster.

```
<aaa_1.3Com> ftp cluster
```

Download the file named aaa.txt from the public TFTP server of the cluster to the member device.

```
<aaa_1.3Com> tftp cluster get aaa.txt
```

Upload the file named bbb.txt from the member device to the public TFTP server of the cluster.

```
<aaa_1.3Com> tftp cluster put bbb.txt
```



- *Upon the completion of the above configurations, you can execute the* ***cluster switch-to*** *{ member-num* | ***mac-address*** *H-H-H } command on the management device to switch to member device view to maintain and manage a member device. You can then execute the* ***cluster switch-to administrator*** *command to resume the management device view.*
- *You can also reboot a member device by executing the* ***reboot member*** *{ member-num* | ***mac-address*** *H-H-H } [* ***eraseflash*** *] command on the management device. For detailed information about these configurations, refer to the preceding description in this chapter.*
- *After the configuration above, on the SNMP host you can receive logs and SMMP trap messages of all the cluster members.*

64 PoE Configuration

PoE Overview

Introduction to PoE

Power over Ethernet (PoE) uses 10BaseT, 100Base-TX, and 1000Base-T twisted pairs to supply power to the remote powered devices (PD) in the network and implement power supply and data transmission simultaneously.

Advantages of PoE

- Reliability: The centralized power supply provides backup convenience, unified management, and safety.
- Easy connection: Network terminals only require an Ethernet cable, but no external power supply.
- Standard: PoE conforms to the 802.3af standard and uses a globally uniform power interfaces;
- Bright application prospect: PoE can be applied to IP phones, wireless access points (APs), chargers for portable devices, module readers, cameras, and data collection.

PoE components

- Power sourcing equipment (PSE): PSE is comprised of the power and the PSE functional module. It can implement PD detection, PD power information collection, PoE, power supply monitoring, and power-off for devices.
- PD: PDs receive power from the PSE. PDs include standard PDs and nonstandard PDs. Standard PDs conform to the 802.3af standard, including IP phones, WLAN APs, network cameras and so on.
- Power interface (PI): PIs are RJ45 interfaces which connect PSE/PDs to network cables.

PoE Features Supported by the Switch 7750

The Switch 7750 supports PoE. Equipped with external power supply and PoE-enabled modules, Switch 7750 can provide -48 VDC power to remote powered devices (PDs) through twisted pairs.

- The Switch 7750 support IEEE802.3af standard. While they can also supply power to PDs noncompliant with the standard.
- The power supply of the Switch 7750 is administered by the main control module; each PoE module on the switch can be viewed as a power sourcing equipment (PSE) and administers the power supply of all the ports on it independently.
- The Switch 7750 can deliver data and current simultaneously through data wires (1, 3, 2, and 6) of category-3/5 twisted pairs.

- The Switch 7750 supply power through the Ethernet electrical ports on the service modules. Each service module can supply power to up to 48 remote devices at the maximum distance of 100 m (328 feet).
- Each Ethernet port can supply at most a power of 15.4 W to remote PDs.
- When the Switch 7750 supply power to remote devices, the maximum total power that it can provide is 2,400 W. The switch determines whether or not to supply power to the next remote PD it discovers depending on the total power it currently supplies.



- *When the PoE-enabled Switch 7750 supply power to remote PDs, the PDs need not have any external power supply.*
- *If a remote PD has an external power supply, the PoE-enabled Switch 7750 and the external power supply will be redundant with each other for the PD.*

External PSE2500-A1 Power System

If PSE2500-A1 power system is taken as the external power supply, the power is distributed as follows:

1 Input voltage: 100 VAC to 140 VAC

- One power supply unit (PSU) of the PSE2500-A1 power system can supply 1,250 W of power, and two PSUs can supply up to 2,400 W of power.
- If the PSUs of PSE2500-A1 power system need to work in redundancy mode, three PSUs are required and they work together to supply 2,400 W of power.

2 Input voltage: 200 VAC to 240 VAC

- One PSU of the PSE2500-A1 power system can supply 2,500 W of power.
- If the PSUs of PSE2500-A1 power system need to work in redundancy mode, two PSUs are required.

PoE-enabled Boards

The following modules of Switch 7750 support PoE:

- 3C16860
- LS81GT48A

Setting PoE Management Mode

Switch 7750 manage PoE in either auto mode or manual mode. Through the setting of the management and PoE priority, the switch determines whether to supply power to newly added PDs when the power supply is almost fully-loaded.

- **auto** mode: When the switch is reaching its full load in supplying power, it will first supply power to the PDs that are connected to the ports with critical priority, and then supply power to the PDs that are connected to the ports with high priority. For example: port A is of critical priority. When the switch is reaching its full load and a new PD is now added to port A, the switch will power down the PD connected to a port with lower priority and turn to supply power to this new PD.
- **manual** mode: When the switch is reaching its full load in supplying power, it will neither take the priority into account nor make change to its original power supply state. For example: Port A has the priority critical. When the switch is reaching its full load and a new PD is now added to port A, the switch will not supply power to this new PD.

*In **auto** mode, when the switch is reaching its full load in supplying power, the switch decides whether to supply power to remote PDs on a port based on the port priority. Note that the switch can compare only the priority of ports on the same module.*

PoE Configuration

PoE Configuration Tasks

Table 579 PoE configuration tasks

Operation	Description	Related section
Configure the PoE feature of a switch	Required	"Configuring the PoE Feature of a Switch" on page 721
Configure the PoE feature of a PoE-enabled board	Required	"Configuring the PoE Feature of a PoE-enabled Board" on page 721
Configure the PoE feature of a PoE port	Required	"Setting the PoE Feature of a PoE Port" on page 722
Upgrade the PSE processing software online	Optional	"Upgrading the PSE Processing Software Online" on page 723

Configuring the PoE Feature of a Switch

Table 580 Configure the PoE feature on a port

Operation	Command	Description
Enter system view	**system-view**	-
Configure the maximum PoE power that a switch can supply	**poe power max-value** *max-value*	Optional By default, the maximum PoE power that a switch can supply is 2,400 W.

*When setting the maximum PoE power supplied by the switch with the **poe power max-value** command, you must set it to a value greater than the total power that has been distributed to the modules. Otherwise, this command cannot be executed successfully. The maximum power that a switch can supply ranges from 37 W to 2,400 W.*

Configuring the PoE Feature of a PoE-enabled Board

Table 581 Configure the PoE feature of a PoE-enabled board

Operation	Command	Description
Enter system view	**system-view**	-
Set the PoE management mode of the switch	**poe power-management** { **auto** | **manual** } **slot** *slot-number*	Optional By default, the switch manages PoE in the **manual** mode.
Enable the PoE feature of the board	**poe enable slot** *slot-number*	Optional By default, the PoE feature is disabled on a module.
Set the maximum power that the module can supply	**poe max-power** *max-power* **slot** *slot-number*	Optional By default, a module provides up to 37W of power.

Table 581 Configure the PoE feature of a PoE-enabled board

Operation	Command	Description
Enable the compatibility detection feature for remote PDs of the board	**poe legacy enable slot** *slot-number*	Optional By default, compatibility detection is disabled for PDs.



- *You can successfully enable PoE on a module only when the remaining power of the switch is not less than the full power of this module.*
- *The required power of PDs may exceed the power configured for them due to their unstable status, thus causing the PDs connected to the last port on the module to be powered off. Therefore, when you configure the maximum power value for a module, ensure enough power for all ports of the module and reserve additional 20 W power for instant high power at the same time.*
- *Once PoE is enabled on a module, the system reserves the power for the slot even after you remove the module from the slot; in this case, you can use the* ***undo poe enable slot*** *command to release this power.*
- *The reserved power for a blank slot will be recycled automatically by the system if you insert a PoE-incapability module into the slot. The reserved power for a blank slot will still be distributed to the slot if you insert a different type of module into the slot and the module is PoE-enabled.*
- *Before you enable the PoE-compatibility detection on a module, you must first enable PoE on this module with the* ***poe enable slot slot-num*** *command.*
- *When PoE-compatibility detection is performed on non-standard devices, the system performance will be affected. When standard 802.3af devices are connected to the module, you are not recommended to enable the PoE-compatibility detection feature.*

Setting the PoE Feature of a PoE Port

Table 582 Set the PoE management mode and PoE priority of a port

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Enable the PoE feature	**poe enable**	Required By default, the PoE feature is enabled on a port when the PoE feature is enabled on a module.
Set the maximum power supplied by the port	**poe max-power** *max-power*	Optional By default, the maximum power supplied by the port is 15.4 W.
Set the power supply mode of the port	**poe mode** { **signal** | **spare** }	Optional The Switch 7750 support only the **signal** mode.
Se the PoE priority of the port	**poe priority** { **critical** | **high** | **low** }	Optional By default, the PoE priority of the port is **low**

- *The Switch 7750 do not support the **spare** mode.*
- *When a module is almost fully loaded and a new PD is added, the switch will respond to the PD according to the PoE management mode. For details, see "Setting PoE Management Mode" on page 720.*
- *In **auto** mode, when the switch is reaching its full load in supplying power, the switch decides whether to supply power to remote PDs on a port based on the port priority. Note that the switch can compare only the priority of ports on the same module.*

Upgrading the PSE Processing Software Online

The online upgrading of PSE processing software can update the processing software or repair the software if it is damaged. After downloading the PSE processing software to the Flash of the switch, you can perform the following configuration. Refer to "File System Management" on page 791 for how to download the PSE processing software.

Table 583 Upgrade PSE processing software online

Operation	Command	Description
Enter system view	**system-view**	-
Upgrade the PSE processing software online	**poe upgrade** { **refresh** | **full** } *filename* **slot** *slot-number*	Required

- *The **refresh** update mode is to upgrade the valid software in the PSE through refreshing the software, while the **full** update mode is to delete the invalid software in PSE completely and then reload the software.*
- *Generally, the **refresh** update mode is used to upgrade the PSE processing software.*
- *When the PSE processing software is damaged (that is, all the PoE commands cannot be successfully executed), you can use the **full** update mode to upgrade and restore the software.*
- *When the upgrading procedure in **refresh** update mode is interrupted for some unexpected reason (such as power-off) or some errors occur, if the upgrade in **full** mode fails after restart, you must upgrade in **full** mode after power-off and restart of the device. In this way, the upgrade procedure succeeds.*

Displaying PoE Configuration

After the above configuration, execute the **display** command in any view to see the operation of the PoE feature and verify the configuration.

Table 584 Display and maintain PoE

Operation	Command	Description
Display the PoE status of a specific port or all ports of the switch	**display poe interface** { *interface-type interface-number* | **all** }	You can execute the **display** command in any view
Display the PoE power information of a specific port or all ports of the switch	**display poe interface power** { *interface-type interface-number* | **all** }	
Display the PSE parameters	**display poe powersupply**	
Display the power supply status of each module and the power that the module supplies	**display poe pse**	

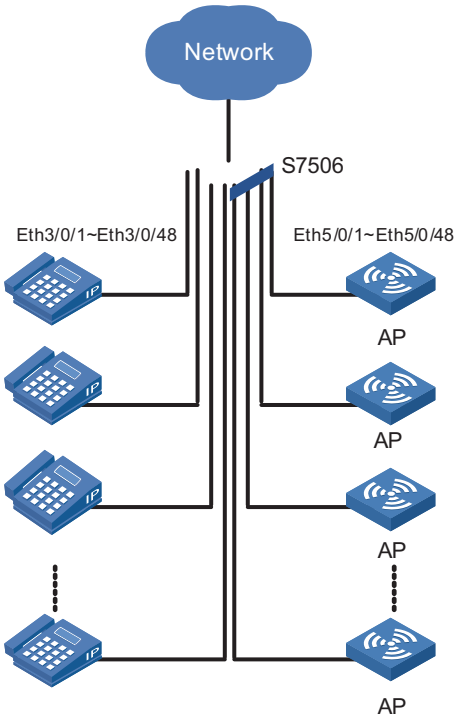
PoE Configuration Example

Networking requirements

- Two PoE-enabled modules are installed in slot 3 and 5 on a Switch 7757.
- Online upgrade the PSE processing software of the PoE module in slot 5 of the Switch 7757.
- Ethernet3/0/1 to Ethernet3/0/48 are connected with IP phones and Ethernet5/0/1 to Ethernet5/0/48 are connected with access point (AP) devices.
- The IP phones are connected to Ethernet3/0/1 through Ethernet3/0/48, and access point (AP) devices are connected to Ethernet5/0/1 through Ethernet5/0/48.
- PoE need not be enabled on the IP phones connected to Ethernet3/0/1 and Ethernet3/0/48.
- Ethernet3/0/48 requires high priority.
- Set the PoE management mode of slot 3 to **auto**.
- Slot 3 is supplied with 400 W of power and slot 5 is supplied with full power (namely, 806 W).
- Enable PoE-compatibility detection on the PoE module in slot 3.
- The input power of the AP device connected the Ehternet5/0/15 port cannot be greater than 9 W.

Networking diagram

Figure 185 Network diagram for PoE



Configuration procedure

Enter system view.

```
<SW7750>system-view
```

Online upgrade the PSE processing software of the PoE module in slot 5 of the Switch 7757.

```
[SW7750] poe upgrade refresh 0400_001.S19
```

Enable the PoE feature on the modules in slot 3 and slot 5.

```
[SW7750] poe enable slot 3
[SW7750] poe enable slot 5
```

Set the PoE management mode on slot 3 to **auto**.

```
[SW7750] poe power-management auto slot 3
```

Set the maximum power supplied by the module in slot 3 to 400 W.

```
[SW7750] poe max-power 400 slot 3
```

Set the maximum power supplied by the module in slot 5 is 806 W (full power).

```
[SW7750] poe max-power 806 slot 5
```

Disable the PoE feature on Ethernet3/0/23 and Ethernet3/0/24.

```
[SW7750]interface Ethernet 3/0/23
[SW7750-Ethernet3/0/23] undo poe enable
[SW7750-Ethernet3/0/23] quit
[SW7750]interface Ethernet 3/0/24
[SW7750-Ethernet3/0/24] undo poe enable
[SW7750-Ethernet3/0/24] quit
```

Set the priority of Ethernet3/0/48 to critical, so that the devices connected to Ethernet3/0/48 can be provided with power preferentially without interrupting power supply to the current ports.

```
[SW7750]interface Ethernet 3/0/48
[SW7750-Ethernet3/0/48] poe priority critical
```

Enable the PoE-compatibility detection feature on the module in slot 3.

```
[SW7750] poe legacy enable slot 3
```

Set the maximum PoE power supplied by Ethernet5/0/15 to 9 W.

```
[SW7750] interface Ethernet5/0/15
[SW7750-Ethernet5/0/15] poe max-power 9000
```

65 POE PSU SUPERVISION CONFIGURATION

Introduction to PoE PSU Supervision

The PoE-enabled Switch 7750 can monitor the external PoE power supply units (PSUs) through Fabrics.

Table 585 PoE PSU supervision configuration tasks

Operation	Description	Related section
Configure AC input alarm thresholds	Required	"AC Input Alarm Thresholds Configuration" on page 727
Configure DC input alarm thresholds	Required	"DC Output Alarm Threshold Configuration" on page 728

The PSE performance will be affected by fast switching of PoE PSUs. The interval of switching PoE PSUs must be no less than 5 seconds.

AC Input Alarm Thresholds Configuration

You can set the AC input alarm thresholds for the PoE PSUs to enable the Switch 7750 to monitor the AC input voltages of the PSUs in real time through Fabrics.

Configuring AC Input Alarm Threshold

Table 586 Configure AC input alarm thresholds

Item	Command	Description
Enter the system view	**system-view**	-
Set the overvoltage alarm threshold of AC input (upper threshold) for the PoE PSUs	**poe-power input-thresh upper** *string*	Required, and the max voltage is 264.0 V.
Set the undervoltage alarm threshold of AC input (lower threshold) for the PoE PSUs	**poe-power input-thresh lower** *string*	Required, and the min voltage is 90.0 V.

- *You can set the thresholds to any appropriate values in the range, but make sure the lower threshold is less than the upper threshold.*
- *For 220 VAC input, it is recommended to set the upper threshold to 264.0 V and the lower threshold to 181.0 V.*
- *For 110 VAC input, you are recommended to set the upper threshold to 132.0 V and the lower threshold to 90.0 V.*

AC Input Alarm Threshold Configuration Example

Network requirements

- Set the overvoltage alarm threshold of AC input for PoE PSUs to 264.0 V.
- Set the undervoltage alarm threshold of AC input for PoE PSUs to 181.0 V.

Configuration procedure

Enter the system view.

```
<SW7750> system-view
```

Set the overvoltage alarm threshold of AC input for PoE PSUs to 264.0 V.

```
[SW7750] poe-power input-thresh upper 264.0
```

Set the undervoltage alarm threshold of AC input for PoE PSUs to 181.0 V.

```
[SW7750] poe-power input-thresh lower 181.0
```

Display the AC input state of the PoE PSUs.

```
[SW7750] display poe-power ac-input state
```

DC Output Alarm Threshold Configuration

You can set the DC output alarm thresholds for the PoE PSUs to enable the Switch 7750 to monitor the DC output voltages of the PSUs in real time through Fabrics.

DC Output Alarm Thresholds Configuration Tasks

Table 587 DC output alarm thresholds configuration task

Operation	Command	Description
Enter the system view	**system-view**	-
Set the overvoltage alarm threshold of DC output (upper threshold) for the PoE PSUs	**poe-power output-thresh upper** *string*	Required You are recommended to set the upper threshold to 47 V when 220 VAC or 110 VAC is input.
Set the undervoltage alarm threshold of DC output (lower threshold) for the PoE PSUs	**poe-power output-thresh lower** *string*	Required You are recommended to set the lower threshold to 55 V when 220 VAC or 110 VAC is input.

DC Output Alarm Threshold Configuration Example

Network requirements

- Set the overvoltage alarm threshold of DC output for the PoE PSUs to 55.0 V.
- Set the undervoltage alarm threshold of DC output for the PoE PSUs to 47.0 V.

Configuration procedure

Enter the system view.

```
<SW7750> system-view
```

Set the overvoltage alarm threshold of DC output for the PoE PSUs to 55.0 V.

```
[SW7750] poe-power output-thresh upper 55.0
```

Set the undervoltage alarm threshold of DC output for the PoE PSUs to 47.0 V.

```
[SW7750] poe-power output-thresh lower 47.0
```

Display the DC output state of the PoE PSUs.

```
[SW7750] display poe-power dc-output state
```

Display the DC output voltage/current values of the PoE PSUs.

```
[SW7750] display poe-power dc-output value
```

Displaying PoE Supervision Information

After the above configuration, you can execute the **display** commands in any view to display the PoE operation of the switch and verify the configuration.

Table 588 Display PoE supervision information

Operation	Command	Description
Display the basic information about the external PoE PSUs.	**display supervision-module information**	You can execute the **display** command in any view
Display alarm information about the PoE PSUs.	**display poe-power alarm**	
Display the number and state of the AC power distribution switches in the external PoE PSUs.	**display poe-power switch state**	
Display the AC input state of the external PoE PSUs	**display poe-power ac-input state**	
Display the DC output of the external PoE PSUs	**display poe-power dc-output state**	
Display the DC output voltage/current values of the external PoE PSUs	**display poe-power dc-output value**	

For details about output information, refer to the *Command Manual*.

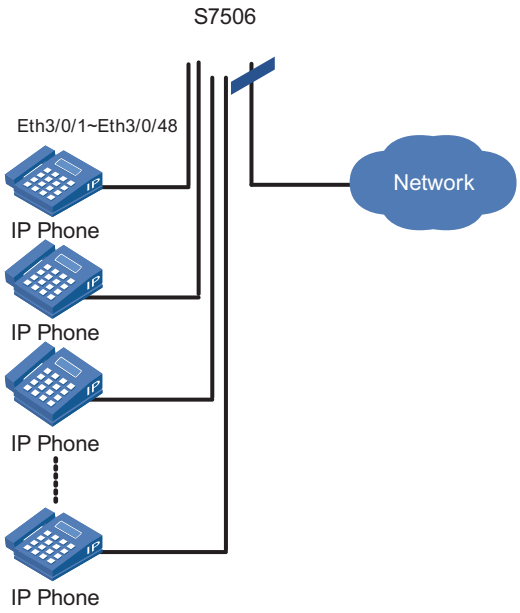
PoE PSU Supervision Configuration Example

Network requirements

- Insert a PoE-enabled module into slot 3 of the Switch 7750.
- Connect IP phones to Ethernet3/0/1 through Ethernet3/0/48.
- Set the AC input and DC output alarm thresholds to appropriate values.

Network diagram

Figure 186 Network diagram for PoE supervision configuration



Configuration procedure

Enter the system view.

```
<SW7750> system-view
```

Enable PoE on the module in slot 3.

```
[SW7750] poe enable slot 3
```

Set the overvoltage alarm threshold of AC input for the PoE PSUs to 264.0 V.

```
[SW7750] poe-power input-thresh upper 264.0
```

Set the undervoltage alarm threshold of AC input for the PoE PSUs to 181.0 V.

```
[SW7750] poe-power input-thresh lower 181.0
```

Set the overvoltage alarm threshold of DC output for the PoE PSUs to 55.0 V.

```
[SW7750] poe-power output-thresh upper 55.0
```

Set the undervoltage alarm threshold of DC output for the PoE PSUs to 47.0 V.

```
[SW7750] poe-power output-thresh lower 47.0
```

66 POE PROFILE CONFIGURATION

Introduction to PoE Profile

On a large-sized network or a network with mobile users, to help network administrators to monitor the PoE features of the switch, Switch 7750 Ethernet switches provide the PoE profile features.

Features of PoE profile:

- Various PoE profiles can be created. PoE policy configurations applicable to different user groups are stored in the corresponding PoE profiles. These PoE profiles can be applied to the ports used by the corresponding user groups.
- When users connect a PD to a PoE-profile-enabled port, the PoE configurations in the PoE profile will be enabled on the port.

PoE Profile Configuration Tasks

Table 589 Configure PoE profile

Operation		Command	Description
Enter system view		**system-view**	-
Create a PoE profile		**poe-profile** *profile-name*	Required Enter PoE profile view while creating the PoE profile
Configure the relevant features in PoE profile	Enable the PoE feature on a port	**poe enable**	Required The PoE feature on a port is enabled by default
	Configure PoE mode for Ethernet ports	**poe mode** { **signal** | **spare** }	Optional By default, the PoE mode is set to **signal**.
	Configure the PoE priority for Ethernet ports	**poe priority** { **critical** | **high** | **low** }	Optional By default, PoE priority is set to **low**.
	Configure the maximum power for Ethernet ports	**poe max-power** *max-power*	Optional By default, the maximum power is set to 15,400 milliwatts.
Return to system view.		**quit**	-

Table 589 Configure PoE profile

Operation			Command	Description
Apply the existing PoE profile to the specified Ethernet port	System view		**apply poe-profile** *profile-name* **interface** *interface-type interface-number* [**to** *interface-type interface-number*]	Required Users can decide whether to configure the settings in system view or port view
	In Ethernet port view:	Enter Ethernet port view	**interface** *interface-type interface-number*	
		Apply the existing PoE profile to the port	**apply poe-profile** *profile-name*	

The following rules should be obeyed

- *A PoE profile is a group of PoE configurations. Multiple PoE features can be set in a PoE profile. When the **apply poe-profile** command applies a PoE profile to a port, some PoE features can be applied successfully while some PoE configurations in it cannot.*
- *When the **apply poe-profile** command is used to apply a PoE profile to a port, the PoE profile is applied successfully if one PoE feature in the PoE profile is applied properly.*
- *If one or more features in the PoE profile are not applied properly on a port, the switch prompts explicitly which PoE features in the PoE profile are not applied properly on which ports.*
- *The **display current-configuration** command can be used to query which PoE profiles are applied to a port. However, the command cannot be used to query which PoE features in a PoE profiles are applied successfully.*

Displaying PoE Profile Configuration

After the above configuration, execute the **display** command in any view to see the running status of the PoE profile. You can verify the configurations by viewing the information.

Table 590 Display the PoE profile configuration

Configuration	Command	Description
Display the detailed information about the PoE profiles created on the switch	**display poe-profile** { **all-profile** | **interface** *interface-type interface-number* | **name** *profile-name* }	The **display** command can be executed in any view

PoE Profile Configuration Example

Network requirements

Ethernet2/0/1 through Ethernet2/0/10 of the Switch 7757 are used by users of group A, who have the following requirements:

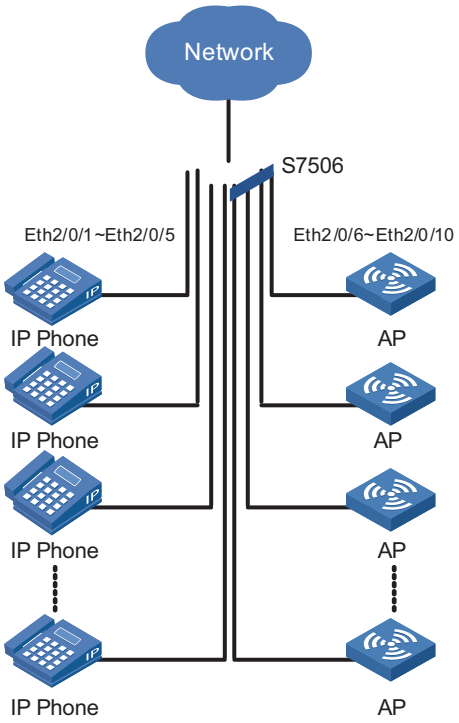
- The PoE function can be enabled on all ports.
- Signal cables are used to supply power.

- The PoE priority for Ethernet2/0/1 through Ethernet2/0/5 is Critical, whereas the PoE priority for Ethernet2/0/6 through Ethernet2/0/10 is High.
- The maximum power for Ethernet2/0/1 through Ethernet2/0/5 ports is 3,000 mW, whereas the maximum power for Ethernet2/0/6 through Ethernet2/0/10 is 15,400 mW.

Based on the above requirements, two PoE profiles are made for users of group A.

- Apply PoE profile 1 for Ethernet2/0/1 through Ethernet 1/0/5;
- Apply PoE profile 2 for Ethernet2/0/6 through Ethernet 1/0/10.

Figure 187 PoE profile application



Configuration procedure

Create Profile1, and enter PoE profile view.

```
<SW7750> system-view
[SW7750] poe-profile Profile1
```

In Profile1, add the PoE policy configuration applicable to Ethernet2/0/1 through Ethernet2/0/5 ports for users of group A.

```
[SW7750-poe-profile-Profile1] poe enable
[SW7750-poe-profile-Profile1] poe mode signal
[SW7750-poe-profile-Profile1] poe priority critical
[SW7750-poe-profile-Profile1] poe max-power 3000
[SW7750-poe-profile-Profile1] quit
```

Display detailed configuration information for Profile1.

```
[SW7750] display poe-profile name Profile1
 Poe-profile: Profile1, 2 action
```

```
 poe max-power 3000
 poe priority critical
```

Create Profile2, and enter poe-profile view.

```
[SW7750] poe-profile Profile2
```

In Profile2, add the PoE policy configuration applicable to Ethernet2/0/6 through Ethernet2/0/10 ports for users of group A.

```
[SW7750-poe-profile-Profile2] poe enable
[SW7750-poe-profile-Profile2] poe mode signal
[SW7750-poe-profile-Profile2] poe priority high
[SW7750-poe-profile-Profile2] poe max-power 15400
[SW7750-poe-profile-Profile2] quit
```

Display detailed configuration information for Profile2.

```
[SW7750] display poe-profile name Profile2
 Poe-profile: Profile2, 1 action
 poe priority high
```

Apply the configured Profile1 to Ethernet2/0/1 through Ethernet2/0/5 ports.

```
[SW7750] apply poe-profile Profile1 interface Ethernet 2/0/1 to Ethernet 2/0/5
```

Apply the configured Profile2 to Ethernet2/0/6 through Ethernet2/0/10 ports.

```
[SW7750] apply poe-profile Profile2 interface Ethernet 2/0/6 to Ethernet 2/0/10
```

67 UDP-HELPER CONFIGURATION

Introduction to UDP-Helper

UDP-Helper is designed to relay specified UDP broadcast packets. It enables a device to operate as a UDP packet relay. That is, it can convert UDP broadcast packets into unicast packets and forward them to a specified server.

Normally, all the received UDP broadcast packets are passed to the UDP module. With the UDP-Helper function enabled, the device checks the destination port numbers of the received UDP broadcast packets and duplicates those with their destination port numbers being that configured for UDP-Helper to the UDP-Helper module. The UDP-helper module in turn modifies the destination IP addresses of the packets and then sends the packet to the specified destination server.



The DHCP Relay module uses UDP port 67 and 68 to relay BOOTP/DHCP broadcast packets, so do not use port 67 and 68 as UDP-Helper destination ports.

With UDP-Helper enabled, the device relays the UDP broadcast packets whose destination ports are one of the six UDP ports list in Table 591 by default.

Table 591 List of default UDP ports

Protocol	UDP port number
Trivial file transfer protocol (TFTP)	69
Domain name system (DNS)	53
Time service	37
NetBIOS name service (NetBIOS-NS)	137
NetBIOS datagram service (NetBIOS-DS)	138
TACACS (terminal access controller access control system)	49

Configuring UDP-Helper

Table 592 Configure UDP-Helper

Operation	Command	Description
Enter system view	**system-view**	-
Enable UDP-Helper	**udp-helper enable**	Required UDP-Helper is disabled by default

Table 592 Configure UDP-Helper

Operation	Command	Description
Configure a UDP port as a UDP-Helper destination port	**udp-helper port** { *port* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }	This operation is unnecessary if the port is among the default UDP ports listed in Table 591. With UDP-Helper enabled, UDP broadcast packets destined for the ports listed in Table 591 are relayed by default.
Enter VLAN interface view	**interface vlan-interface** *vlan-id*	-
Configure the destination server to which the matched UDP broadcast packets are to be forwarded	**udp-helper server** *ip-address*	Required By default, no destination server is configured

CAUTION:

- *You need to enable the UDP-Helper function before specifying a UDP-Helper destination port.*
- *The **dns**, **netbios-ds**, **netbios-ns**, **tacacs**, **tftp**, and **time** keywords refers to the six default UDP ports. You can configure a default port to be a UDP-Helper destination port by specifying the corresponding port number or the corresponding keyword. For example, **udp-helper port** 53 and **udp-helper port dns** specify the same port as a UDP-Helper destination port.*
- *The **display current-configuration** command does not display the default UDP ports that are configured to be UDP-Helper destination ports.*
- *After UDP-Helper is disabled, all the configured UDP ports are cancelled, including the default ports.*
- *You can configure up to 20 destination servers on a VLAN interface.*
- *If the destination server is configured on a VLAN interface, the UDP broadcast packets received from the ports in the VLAN with specific UDP-Helper destination ports are forwarded to the destination server configured on the VLAN interface.*

Displaying and Maintaining UDP-Helper

After performing the above configurations, you can use the **display** command in any view to display the information about the destination servers and the number of the packets forwarded to each destination server. Verify the configuration by checking the output information. You can use the **reset** command in user view to clear statistics about packets forwarded by UDP-Helper.

Table 593 Display and Maintain UDP-Helper

Operation	Command	Description
Display the information about the destination servers and the number of the packets forwarded to each destination server	**display udp-helper server** [**interface vlan-interface** *vlan-id*]	You can use the **display** command in any view

Table 593 Display and Maintain UDP-Helper

Operation	Command	Description
Clear the statistics about packets forwarded by UDP-Helper	**reset udp-helper packet**	You can use the **reset** command in user view

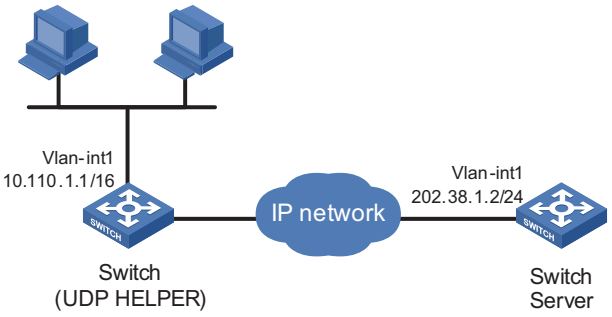
UDP-Helper Configuration Example

Network requirements

The IP address of VLAN 1 interface is 10.110.1.1/16. The VLAN interface is connected to the network segment 10.110.0.0/16. Configure to forward the broadcast UDP packets whose destination UDP port number is 55 to the server with its IP address being 202.38.1.2/24.

Network diagram

Figure 188 Network diagram for UDP-Helper configuration



Configuration procedure

This example assumes that the route between the switch and the network segment 202.38.1.0/24 is reachable.

Enable UDP-Helper.

```
<SW7750> system-view
[SW7750] udp-helper enable
```

Configure port 55 as a UDP-Helper destination port.

```
[SW7750] udp-helper port 55
```

Configure the server with the IP address of 202.38.1.2 as a destination server for the UDP broadcast packets.

```
[SW7750] interface Vlan-interface 1
[SW7750-Vlan-interface1] ip address 10.110.1.1 16
[SW7750-Vlan-interface1] udp-helper server 202.38.1.2
```

68 SNMP CONFIGURATION

SNMP Overview

By far, the simple network management protocol (SNMP) has gained the most extensive application in the computer networks. SNMP has been put into use and widely accepted as an industry standard in practice. It is used for ensuring the transmission of the management information between any two nodes. In this way, network administrators can easily search and modify the information on any node on the network. In the meantime, they can locate faults promptly and implement the fault diagnosis, capacity planning and report generating.

SNMP adopts the polling mechanism and provides the most basic function set. It is most applicable to the small-sized, fast-speed and low-cost environment. It only requires the connectionless transport layer protocol UDP; and is thus widely supported by many products.

SNMP Operation Mechanism

SNMP can be divided into two parts, namely, Network Management Station and Agent:

Network management station (NMS) is the workstation for running the client program. At present, the commonly used NM platforms include 3Com's Network Management Products, Sun NetManager and IBM NetView.

Agent is the server software operated on network devices.

The NMS can send GetRequest, GetNextRequest and SetRequest messages to the Agent. Upon receiving the requests from the NMS, Agent will perform Read or Write operation according to the message types, generate and return the Response message to the NMS.

Agent will send Trap message on its own initiative to the NMS to report the events whenever the device status changes or the device encounters any abnormalities such as restarting the device.

SNMP Versions

Currently SNMP Agent of the device supports SNMP V3, and is compatible with SNMP V1 and SNMP V2C.

SNMP V3 adopts user name and password authentication.

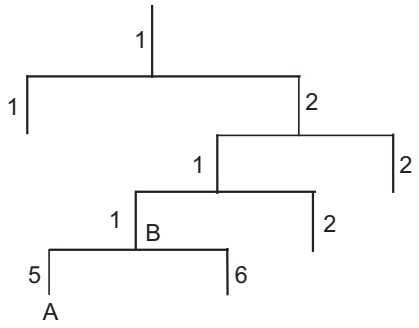
SNMP V1 and SNMP V2C adopt community name authentication. The SNMP packets failing to pass community name authentication are discarded. The community name is used to define the relation between SNMP NMS and SNMP Agent. The community name can limit access to SNMP Agent from SNMP NMS, functioning as a password. You can define the following features related to the community name.

- Define MIB view that a community can access.
- Set read-only or read-write right to access MIB objects for the community. The read-only community can only query device information, while the read-write community can configure the device.
- Set the basic ACL specified by the community name.

MIBs Supported by the Device

The management variable in the SNMP packet is used to describe management objects of a device. To uniquely identify the management objects of the device in SNMP messages, SNMP adopts the hierarchical naming scheme to identify the managed objects. It is like a tree, and each tree node represents a managed object, as shown in Figure 189. Thus the object can be identified with the unique path starting from the root.

Figure 189 Architecture of the MIB tree



The management information base (MIB) is used to describe the hierarchical architecture of the tree and it is the set defined by the standard variables of the monitored network device. In the above figure, the managed object B can be uniquely specified by a string of numbers {1.2.1.1}. The number string is the Object Identifier of the managed object.

The common MIBs supported by the system are listed in Table 594.

Table 594 Common MIBs

MIB attribute	MIB content	References
Public MIB	MIB II based on TCP/IP network device	RFC1213
	BRIDGE MIB	RFC1493
		RFC2675
	RIP MIB	RFC1724
	RMON MIB	RFC2819
	Ethernet MIB	RFC2665
	OSPF MIB	RFC1253
	IF MIB	RFC1573

Table 594 Common MIBs

MIB attribute	MIB content	References
Private MIB	DHCP MIB	-
	DHCP MIB	
	QACL MIB	
	ADBM MIB	
	IGMP Snooping MIB	
	RSTP MIB	
	VLAN MIB	
	Device management	
	Interface management	
	QACL MIB	-
	ADBM MIB	-
	RSTP MIB	-
	VLAN MIB	-
	Device management	-
	Interface management	-

Configuring SNMP Basic Functions

The configuration of SNMP V3 configuration is different from that of SNMP V1 and SNMP V2C, therefore SNMP basic function configurations for different versions are introduced respectively. For specific configurations, refer to Table 595 and Table 596.

Table 595 Configure SNMP basic functions for SNMP V1 and SNMP V2C

Operation	Command	Description
Enter system view	**system-view**	-
Enable SNMP Agent	**snmp-agent**	Optional By default, SNMP Agent is disabled To enable SNMP Agent, you can execute this command or those commands used to configure SNMP Agent features
Set system information	**snmp-agent sys-info** { **contact** *sys-contact* | **location** *sys-location* | **version** { { **v1** | **v2c** | **v3** }* | **all** } }	Required By default, the contact information for system maintenance is "3Com Corporation", the system location is "Marlborough, MA", and the SNMP version is SNMP V3

Table 595 Configure SNMP basic functions for SNMP V1 and SNMP V2C

Operation			Command	Description
Set a community name and access authority	Direct configuration	Set a community name	**snmp-agent community** { **read** | **write** } *community-name* [**acl** *acl-number* | **mib-view** *view-name*]*	Required ■ Direct configuration for SNMP V1 and SNMP V2C is based on community name ■ Indirect configuration. The added user is equal to the community name for SNMPV1 and SNMPV2C ■ You can choose either of them as needed
	Indirect configuration	Set an SNMP group	**snmp-agent group** { **v1** | **v2c** } *group-name* [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number*]	
		Add a new user for an SNMP group	**snmp-agent usm-user** { **v1** | **v2c** } *user-name group-name* [**acl** *acl-number*]	
Set the maximum size of SNMP packets that the Agent can send/receive			**snmp-agent packet max-size** *byte-count*	Optional By default, it is 2,000 bytes.
Set the device switch fabric ID			**snmp-agent local-switch fabricid** *switch fabricid*	Optional By default, the device switch fabric ID is "Enterprise Number + device information".
Create or update the view information			**snmp-agent mib-view** { **included** | **excluded** } *view-name oid-tree*	Optional By default, the view name is ViewDefault and OID is 1.

Table 596 Configure SNMP basic functions (SNMP V3)

Operation	Command	Description
Enter system view	**system-view**	-
Enable SNMP Agent	**snmp-agent**	Required By default, SNMP Agent is disabled You can enable SNMP agent by executing this command or any configuration command of snmp-agent
Set system information	**snmp-agent sys-info** { **contact** *sys-contact* | **location** sys-l*ocation* | **version** { { **v1** | **v2c** | **v3** }* | **all** } }	Optional By default, the contact information for system maintenance is "Hangzhou 3Com Technologies Co., Ltd.", the system location is "Marlborough, MA", and the SNMP version is SNMP V3.
Set an SNMP group	**snmp-agent group v3** *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number*]	Required

Table 596 Configure SNMP basic functions (SNMP V3)

Operation	Command	Description
Add a new user for an SNMP group	**snmp-agent usm-user v3** *user-name group-name* [**authentication-mode** { **md 5** | **sha** } *auth-password* [**privacy-mode des56** *priv-password*]] [**acl** *acl-number*]	Required
Set the size of SNMP packet that the Agent can send/receive	**snmp-agent packet max-size** *byte-count*	Optional By default, it is 2,000 bytes.
Set the device switch fabric ID	**snmp-agent local-switch fabricid** *switch fabricid*	Optional By default, the device switch fabric ID is "Enterprise Number + device information".
Create or update the view information	**snmp-agent mib-view** { **included** | **excluded** } *view-name oid-tree*	Optional By default, the view name is ViewDefault and OID is 1.

Configuring Trap

Trap is the information that the managed device initiatively sends to the NMS without request. Trap is used to report some urgent and important events (e.g., the managed device is rebooted).

Configuration Prerequisites

Complete SNMP basic configuration.

Configuration Tasks

Table 597 Configure Trap

Operation		Command	Description
Enter system view		**system-view**	-
Enable the device to send Trap packets		**snmp-agent trap enable** [**bgp** [**backwardtransition** | **established**]* | **configuration** | **flash** | **ospf** [*process-id*] [*ospf-trap-list*] | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**]* | **system** | **vrrp** [**authfailure** | **newmaster**]]	Optional By default, the port or the interface is enabled to send Trap packets.
Enable the port to send Trap packets	Enter port view or interface view	**interface** *interface-type interface-number*	
	Enable the port or interface to send Trap packets	**enable snmp trap updown**	
	Quit to system view	**quit**	

Table 597 Configure Trap

Operation	Command	Description
Set Trap target host address	**snmp-agent target-host trap address udp-domain** { *ip-address* } [**udp-port** *port-number*] **params securityname** *security-string* [**v1** | **v2c** | **v3** {**authentication** | **privacy** }]	Required
Set the source address to send Trap packets	**snmp-agent trap source** *interface-type interface-number*	Optional
Set the information queue length of Trap packet sent to destination host	**snmp-agent trap queue-size** *size*	Optional The default value is 100.
Set aging time for Trap packets	**snmp-agent trap life** *seconds*	Optional The default aging time for Trap packets is 120 seconds.
Extend the bound variables in a linkup/linkdown trap packet, that is, add two objects "ifDescr" (interface description) and "ifType" (interface type)	**snmp-agent trap ifmib link extended**	Optional By default, the bound variables in a linkup/linkdown packet are as the standard format defined in IF-MIB.

*The **snmp-agent trap ifmib** command is used to privately extend a linkup/linkdown trap packet and add two objects "ifDescr" (interface description) and "ifType" (interface type) to a trap packet. The two objects facilitate your understanding and failure port location.*

Displaying SNMP

After the above configuration is completed, execute the **display** command in any view to view the running status of SNMP, and to verify the configuration.

Table 598 Display SNMP

Operation	Command	Description
Display system information of the current SNMP device	**display snmp-agent sys-info** [**contact** | **location** | **version**]*	The **display** command can be executed in any view
Display SNMP packet statistics information	**display snmp-agent statistics**	
Display the switch fabric ID of the current device	**display snmp-agent** { **local-switch fabricid** | **remote-switch fabricid** }	
Display group information about the device	**display snmp-agent group** [*group-name*]	
Display SNMP user information	**display snmp-agent usm-user** [**switch fabricid** *switch fabricid* | **username** *user-name* | **group** *group-name*]	
Display the currently configured community name	**display snmp-agent community** [**read** | **write**]	
Display the currently configured MIB view	**display snmp-agent mib-view** [**exclude** | **include** | **viewname** *view-name*]	

SNMP Configuration Example

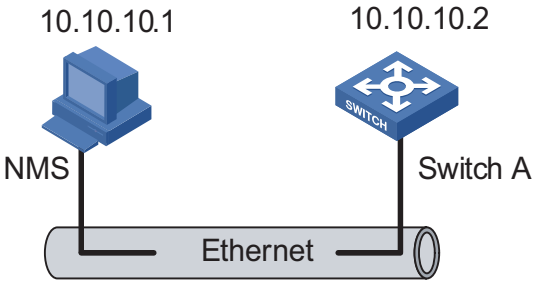
SNMP Configuration Example

Network requirements

- An NMS and Switch A are connected through the Ethernet. The IP address of the NMS is 10.10.10.1 and that of the VLAN interface on Switch A is 10.10.10.2.
- Perform the following configuration on Switch A: setting the community name and access authority, administrator ID, contact and switch location, and enabling the switch to sent trap packet.

Network diagram

Figure 190 Network diagram for SNMP



Network procedure

Set the community name, group name and user.

```
<SW7750> system-view
[SW7750] snmp-agent
[SW7750] snmp-agent sys-info version all
[SW7750] snmp-agent community write public
[SW7750] snmp-agent mib-view include internet 1.3.6.1
[SW7750] snmp-agent group v3 managev3group write-view internet
[SW7750] snmp-agent usm-user v3 managev3user managev3group
```

Set the VLAN interface 2 as the interface used by NMS. Add port Ethernet1/0/2 to VLAN 2. This port will be used for network management. Set the IP address of VLAN interface 2 as 10.10.10.2.

```
[SW7750] vlan 2
[SW7750-vlan2] port Ethernet 1/0/2
[SW7750-vlan2] quit
[SW7750] interface Vlan-interface 2
[SW7750-Vlan-interface2] ip address 10.10.10.2 255.255.255.0
[SW7750-Vlan-interface2] quit
```

Enable the SNMP agent to send Trap packets to the NMS whose IP address is 10.10.10.1. The SNMP community is public.

```
[SW7750] snmp-agent trap enable standard authentication
[SW7750] snmp-agent trap enable standard coldstart
[SW7750] snmp-agent trap enable standard linkup
[SW7750] snmp-agent trap enable standard linkdown
[SW7750] snmp-agent target-host trap address udp-domain 10.10.10.1 u
dp-port 5000 params securityname public
```

Configuring NMS

The Switch 7750 supports 3Com's 3Com's Network Management Products NMS. SNMP V3 adopts user name and password authentication. In [Quidview Authentication Parameter], you need to set a user name, choose security level, and set authorization mode, authorization password, encryption mode, and encryption password respectively according to different security levels. In addition, you must set timeout time and retry times.

You can query and configure the Ethernet switch through the NMS. For more information, refer to the manuals of 3Com's NMS products.



NMS configuration must be consistent with device configuration; otherwise, the NMS cannot manage the device.

69 RMON CONFIGURATION

Introduction to RMON

Remote monitoring (RMON) is a kind of management information base (MIB) defined by Internet Engineering Task Force (IETF) and is a most important enhancement made to MIB II standards. RMON is mainly used to monitor the data traffic across a network segment or even the entire network, and is currently a commonly used network management standard.

An RMON system comprises of two parts: the network management station (NMS) and the agents running on each network device. RMON agents operate on network monitors or network probes to collect and keep track of the statistics of the traffic across the network segments to which their ports connect such as the total number of the packets on a network segment in a specific period of time and the total number of packets that are sent to a specific host successfully.

RMON is fully based on simple network management protocol (SNMP) architecture. It is compatible with the current SNMP, so that you can implement RMON without modifying SNMP. RMON enables SNMP to monitor remote network devices more effectively and actively, thus providing a satisfactory means of monitoring the operation of the subnet. With RMON, the communication traffic between NMS and agents is reduced, thus facilitating the management of large-scale internetworks.

Working Mechanism of RMON

RMON allows multiple monitors. It collects data in one of the following two ways:

- Using the dedicated RMON probe. When an ROM system operates in this way, the NMS directly obtains management information from the RMON probes and controls the network resources. In this case, all information in the RMON MIB can be obtained.
- Embedding RMON agents into network devices (such as routers, switches and hubs) directly to make the latter capable of RMON probe functions. When an RMON system operates in this way, the NMS collects network management information by exchanging information with the SNMP agents using the basic SNMP commands. However, this way depends on device resources heavily and an NMS operating in this way can only obtain four groups of information (instead of all the information in the RMON MIB). The four groups are alarm group, event group, history group and statistics group.

A Switch 7750 implements RMON in the second way. With the embedded RMON agent, the Switch 7750 can serve as a network device with the RMON probe function. Through the RMON-capable SNMP agents running on the Ethernet switch, an NMS can obtain the information about the total traffic, error statistics and performance statistics of the network segments to which the ports of the managed network devices are connected. Thus, the NMS can further manage the networks.

Commonly Used RMON Groups

Event group

The event group is used to define the indexes of events and the processing methods of the events. The events defined in an event group are mainly used in alarm group and extended alarm group to trigger alarms.

You can specify a network device to act in one of the following ways in response to an event:

- Logging the event
- Sending trap messages to the NMS
- Logging the event and sending trap messages to the NMS
- No processing

Alarm group

RMON alarm management enables monitors on specific alarm variables (such as the statistics of a port). When the value of a monitored variable exceeds the threshold, an alarm event is generated, which triggers the network device to act in the set way. Events are defined in event groups.

With an alarm entry defined in an alarm group, a network device performs the following operations accordingly:

- Sampling the defined alarm variables (alarm-variable) once in each specified period (sampling-time)
- Comparing the sampled value with the set threshold and triggering the corresponding events if the sampled value exceeds the threshold

Extended alarm group

With extended alarm entry, you can perform operations on the samples of an alarm variable and then compare the operation result with the set threshold, thus implement more flexible alarm functions.

With an extended alarm entry defined in an extended alarm group, the network devices perform the following operations accordingly:

- Sampling the alarm variables referenced in the defined extended alarm expressions once in each specified period
- Performing operations on sampled values according to the defined operation formulas
- Comparing the operation result with the set threshold and triggering corresponding events if the operation result exceeds the threshold.

History group

After a history group is configured, the Ethernet switch collects network statistics information periodically and stores the statistics information temporarily for later retrieval. A history group can provide the history data of the statistics on network segment traffic, error packets, broadcast packets, and bandwidth utilization.

With the history data management function, you can configure network devices, such as collecting history data, collecting the data of a specific port periodically and saving them.

Statistics group

Statistics group contains the statistics of each monitored port on a network device. An entry in a statistics group is an accumulated value counting from the time when the statistics group is created.

The statistics include the number of the following items: collisions, packets with cyclic redundancy check (CRC) errors, undersize (or oversize) packets, broadcast packets, multicast packets, and received bytes and packets.

With the RMON statistics management function, you can monitor the usage of a port and make statistics on the errors occurred when the ports are being used.

RMON Configuration

Configuration Prerequisites

Before performing RMON configuration, make sure the SNMP agents are correctly configured. For the information about SNMP agent configuration, refer to "Configuring SNMP Basic Functions" on page 741.

Configuring RMON

Table 599 Configure RMON

Operation	Command	Description
Enter system view	**system-view**	-
Add an event entry	**rmon event** *event-entry* [**description** *string*] { **log** | **trap** *trap-community* | **log-trap** *log-trapcommunity* | **none** } [**owner** *text*]	Optional
Add an alarm entry	**rmon alarm** *entry-number alarm-variable sampling-time* { **delta** | **absolute** } **rising threshold** *threshold-value1 event-entry1* **falling threshold** *threshold-value2 event-entry2* [**owner** *text*]	Optional Before adding an alarm entry, you need to use the **rmon event** command to define the event referenced by the alarm entry.
Add an extended alarm entry	**rmon prialarm** *entry-number prialarm-formula prialarm-des sampling-timer* { **delta** | **absolute** | **changeratio** } **rising_threshold** *threshold-value1 event-entry1* **falling_threshold** *threshold-value2 event-entry2* **entrytype** { **forever** | **cycle** *cycle-period* } [**owner** *text*]	Optional Before adding an extended alarm entry, you need to use the **rmon event** command to define the event referenced by the extended alarm entry.
Enter Ethernet port view	**interface** *interface-type interface-number*	-
Add a history entry	**rmon history** *entry-number* **buckets** *number* **interval** *sampling-interval* [**owner** *text*]	Optional

Table 599 Configure RMON

Operation	Command	Description
Add a statistics entry	**rmon statistics** *entry-number* [**owner** *text*]	Optional

- *The **rmon alarm** and **rmon prialarm** commands take effect on existing nodes only.*
- *For each port, only one RMON statistics entry can be created. That is, if an RMON statistics entry is already created for a given port, creation of another entry with a different index for the same port will not succeed.*

Displaying RMON

After the above configuration, you can execute the **display** command in any view to display the RMON running status, and verify the effect of the configuration.

Table 600 Display RMON

Operation	Command	Description
Display RMON statistics	**display rmon statistics** [*interface-type interface-number*]	The **display** command can be executed in any view
Display RMON history information	**display rmon history** [*interface-type interface-number*]	
Display RMON alarm information	**display rmon alarm** [*entry-number*]	
Display extended RMON alarm information	**display rmon prialarm** [*prialarm-entry-number*]	
Display RMON events	**display rmon event** [*event-entry*]	
Display RMON event logs	**display rmon eventlog** [*event-entry*]	

RMON Configuration Example

Network requirements

- Ensure that the SNMP agents are correctly configured before performing RMON configuration.
- The switch to be tested has a configuration terminal connected to its console port and is connected to a remote NMS through Internet. Create an entry in the Ethernet statistics table to make statistics on the Ethernet port performance for network management.

Network diagram

Figure 191 Network diagram for RMON configuration



Configuration procedures

Configure RMON.

```
<SW7750> system-view
[SW7750] interface Ethernet2/0/1
[SW7750-Ethernet2/0/1] rmon statistics 1 owner user1-rmon
```

View RMON configuration.

```
[SW7750-Ethernet2/0/1] display rmon statistics Ethernet2/0/1
Statistics entry 1 owned by user1-rmon is VALID.
  Interface : Ethernet2/0/1<ifIndex.4227626>
  etherStatsOctets         : 0         , etherStatsPkts          : 0
  etherStatsBroadcastPkts  : 0         , etherStatsMulticastPkts : 0
  etherStatsUndersizePkts  : 0         , etherStatsOversizePkts  : 0
  etherStatsFragments      : 0         , etherStatsJabbers       : 0
  etherStatsCRCAlignErrors : 0         , etherStatsCollisions    : 0
  etherStatsDropEvents (insufficient resources): 0
  Packets received according to length (etherStatsPktsXXXtoYYYOctets):
  64     : 0         ,  65-127  : 0         ,  128-255  : 0
  256-511: 0         ,  512-1023: 0         ,  1024-max: 0
```

70 NTP CONFIGURATION

Introduction to NTP

Network time protocol (NTP) is a time synchronization protocol defined by RFC1305. It is used for time synchronization among a set of distributed time servers and clients. NTP transmits packets through UDP port 123.

NTP is intended for time synchronization of all devices that have clocks in a network, so that the clocks of all devices can keep consistent. This enables the applications that require unified time.

A system running NTP not only can be synchronized by other clock sources, but also can serve as a clock source to synchronize other clocks. Besides, it can synchronize, or be synchronized by other systems by exchanging NTP packets.

Applications of NTP

NTP is mainly applied to synchronizing the clocks of all the network devices in a network. For example:

- In network management, the analysis of the log information and debugging information collected from different devices is meaningful and valid only when network devices that generate the information adopts the same time.
- The accounting system requires that the clocks of all the network devices be consistent.
- Some functions, such as restarting all the network devices in a network simultaneously require that they adopt the same time.
- When multiple systems cooperate to handle a rather complex event, to ensure a correct execution order, they must adopt the same time.
- To perform incremental backup operations between a backup server and a host, you must make sure they adopt the same time.

As setting the system time manually in a network with many devices leads to a lot of workload and cannot ensure the accuracy, it is unfeasible for an administrator to perform the operation. However, an administrator can synchronize the devices in a network with required accuracy by performing NTP configuration.

NTP benefits from the following advantages:

- Defining the accuracy of clocks by strata to synchronize the time of all the devices in a network quickly
- Supporting access control and MD5 authentication
- Sending protocol packets in unicast, multicast or broadcast mode



The accuracy of a clock is determined by its stratum, which ranges from 1 to 16. The stratum of the reference clock ranges from 1 to 15. The accuracy descends

with the increasing of stratum number. The clocks with the stratum of 16 are in unsynchronized state and cannot serve as reference clocks.

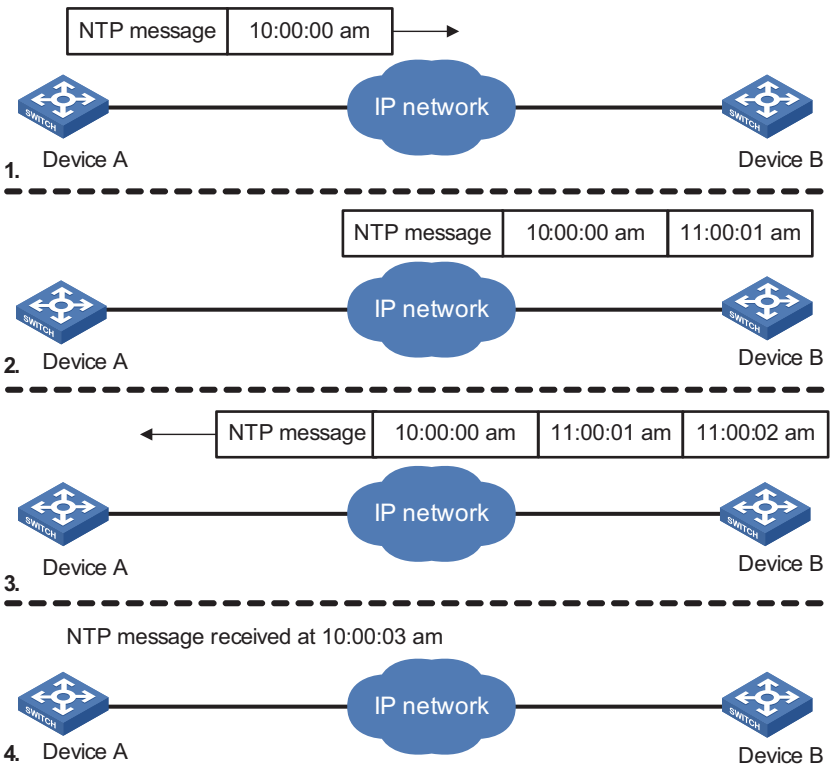
Working Principle of NTP

Figure 192 shows the implementation principle of NTP.

Ethernet switch A (Device A) is connected to Ethernet switch B (Device B) through Ethernet ports. Both having their own system clocks, they need to synchronize the clocks of each other through NTP. To help you to understand the implementation principle, we suppose that:

- Before the system clocks of Device A and Device B are synchronized, the clock of Device A is set to 10:00:00 am, and the clock of Device B is set to 11:00:00 am.
- Device B serves as the NTP server, that is, the clock of Device A will be synchronized to that of Device B.
- It takes one second to transfer an NTP message from Device A to Device B or from Device B to Device A.

Figure 192 Implementation principle of NTP



The procedure of synchronizing the system clock is as follows:

- Device A sends an NTP message to Device B, with a timestamp 10:00:00 am (T_1) identifying when it is sent.
- When the message arrives at Device B, Device B inserts its own timestamp 11:00:01 am (T_2) into the packet.
- When the NTP message leaves Device B, Device B inserts its own timestamp 11:00:02 am (T_3) into the packet.

- When receiving a response packet, the local time of Device A is 10:00:03 am (T4).

At this time, Device A has enough information to calculate the following two parameters:

- Delay for an NTP message to make a round trip between Device A and Device B:

  Delay = $(T_4 - T_1) - (T_3 - T_2)$.

- Time offset of Device A relative to Device B:

  Offset = $((T_2 - T_1) + (T_3 - T_4))/2$.

Device A can then set its own clock according to the above information to synchronize its clock to that of Device B.

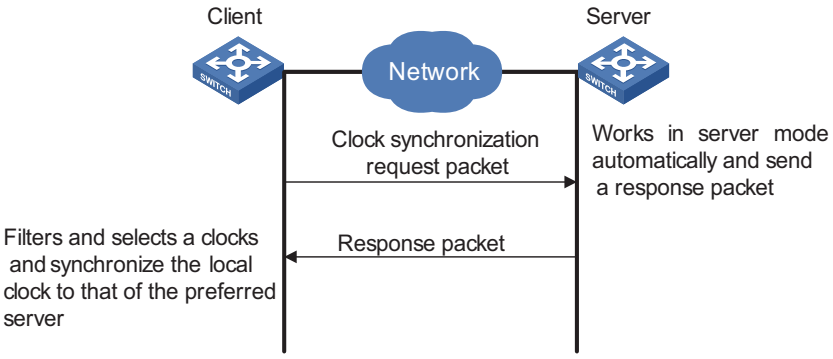
For detailed information, refer to RFC 1305.

NTP Implementation Mode

To accommodate networks of different structures and switches in different network positions, NTP can operate in multiple modes, as described in the following.

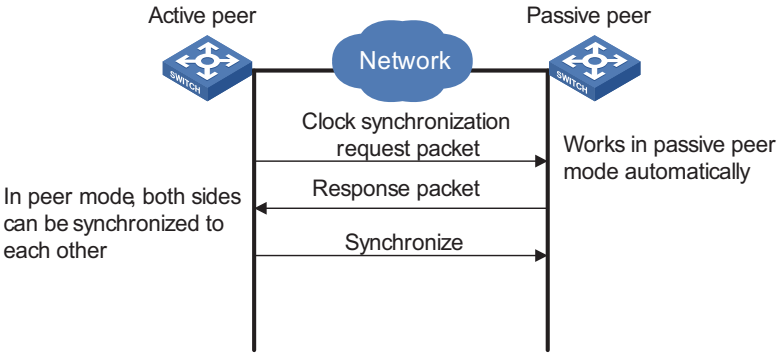
Client/Server mode

Figure 193 NTP implementation mode: client/Sever mode



Peer mode

Figure 194 NTP implementation mode: peer mode

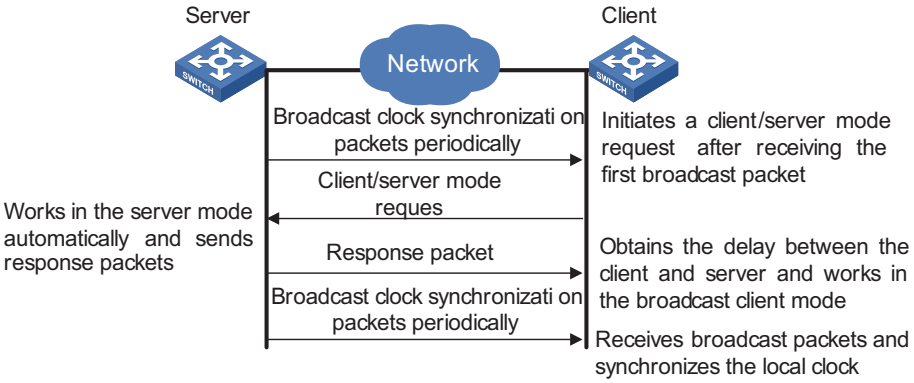


In peer mode, the active peer sends clock synchronization packets first, and its peer works as a passive peer automatically.

If both of the peers have reference clocks, the one with smaller stratum is adopted.

Broadcast mode

Figure 195 NTP implementation mode: broadcast mode



Multicast mode

Figure 196 NTP implementation mode: multicast mode

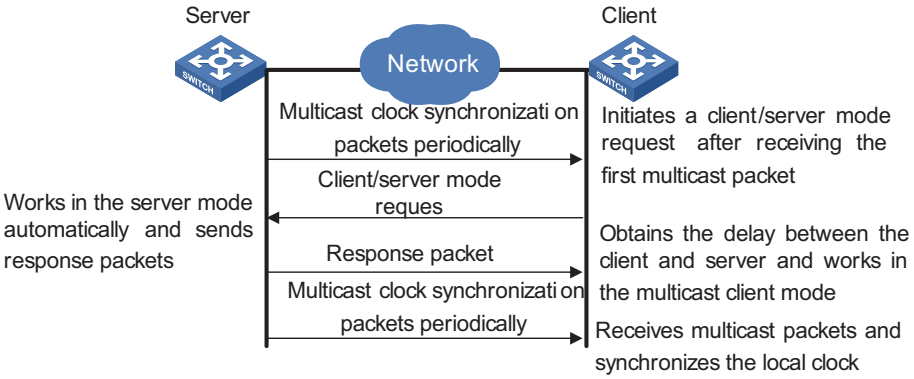


Table 601 describes how the above mentioned NTP modes are implemented on a Switch 7750.

Table 601 NTP implementation modes on a Switch 7750

NTP implementation mode	Configuration on Switch 7750
Client/Server mode	Configure the Switch 7750 to operate in the NTP server mode. In this case, the remote server operates as the local time server, and the Switch 7750 operates as the client.
Peer mode	Configure the Switch 7750 to operate in NTP peer mode. In this case, the remote server operates as the peer of the Switch 7750, and the Switch 7750 operates as the active peer.

Table 601 NTP implementation modes on a Switch 7750

NTP implementation mode	Configuration on Switch 7750
Broadcast mode	■ Configure the Switch 7750 to operate in NTP broadcast server mode. In this case, the Switch 7750 broadcasts NTP packets through the VLAN interface configured on the switch. ■ Configure the Switch 7750 to operate in NTP broadcast client mode. In this case, the Switch 7750 receives broadcast NTP packets through the VLAN interface configured on the switch.
Multicast mode	■ Configure the Switch 7750 to operate in NTP multicast server mode. In this case, the Switch 7750 sends multicast NTP packets through the VLAN interface configure on the switch. ■ Configure the Switch 7750 to operate in NTP multicast client mode. In this case, the Switch 7750 receives multicast NTP packets through the VLAN interface configure on the switch.

NTP Implementation Mode Configuration

A switch can operate in the following NTP modes:

- NTP client mode
- NTP server mode
- NTP peer mode
- NTP broadcast server mode
- NTP broadcast client mode
- NTP multicast server mode
- NTP multicast client mode

Prerequisites

When a Switch 7750 operates in NTP server mode or NTP peer mode, you need to perform configuration on the client or the active peer only. When a Switch 7750 operates in NTP broadcast mode or NTP multicast mode, you need to perform configurations on both the server side and the client side.

Configuring NTP Implementation Modes

Table 602 Configure NTP implementation modes

Operation	Command	Description
Enter system view	**system-view**	-
Configure to operate in the NTP client mode	**ntp-service unicast-server** { *remote-ip* | *server-name* } [**authentication-keyid** *key-id* | **priority** | **source-interface** *interface -type interface-number* | **version** *number*]*	Optional By default, no Ethernet switch operates in the NTP client mode
Configure to operate in the NTP peer mode	**ntp-service unicast-peer** { *remote-ip* | *peer-name* } [**authentication-keyid** *key-id* | **priority** | **source-interface** *interface -type interface-number* | **version** *number*]*	Optional By default, no Ethernet switch operates in the NTP peer mode

Table 602 Configure NTP implementation modes

Operation	Command	Description
Enter VLAN interface view	**interface** *interface -type interface-number*	-
Configure to operate in the NTP broadcast client mode	**ntp-service broadcast-client**	Optional By default, no Ethernet switch operates in the NTP broadcast client mode
Configure to operate in the NTP broadcast server mode	**ntp-service broadcast-server** [**authentication-keyid** *key-id* | **version** *number*]*	Optional By default, no Ethernet switch operates in the NTP broadcast server mode
Configure to operate in the NTP multicast client mode	**ntp-service multicast-client** [*ip-address*]	Optional By default, no Ethernet switch operates in the NTP multicast client mode
Configure to operate in the NTP multicast server mode	**ntp-service multicast-server** [*ip-address*] [**authentication-keyid** *keyid* | **ttl** *ttl-number* | **version** *number*]*	Optional By default, no Ethernet switch operates in the NTP multicast server mode

NTP client mode

When a Switch 7750 operates in the NTP client mode,

- The remote server identified by the *remote-ip* argument operates as the NTP time server. The Switch 7750 operates as the client, whose clock is synchronized to the NTP server. (In this case, the clock of the NTP server is not synchronized to the local client.)
- When the *remote-ip* argument is an IP address of a host, it cannot be a broadcast or a multicast address, neither can it be the IP address of a reference clock.

NTP peer mode

When a Switch 7750 operates in NTP peer mode,

- The remote server identified by the *remote-ip* argument operates as the peer of the Switch 7750, and the Switch 7750 operates as the active peer. The clock of the Switch 7750 can be synchronized to the remote server or be used to synchronize the clock of the remote server.
- When the *remote-ip* argument is an IP address of a host, it cannot be a broadcast or a multicast address, neither can it be the IP address of a reference clock.

NTP broadcast server mode

When a Switch 7750 operates in NTP broadcast server mode, it broadcasts a clock synchronization packet periodically. The devices which are configured to be in the NTP broadcast client mode will respond this packet and start the clock synchronization procedure.

NTP multicast server mode

When a Switch 7750 operates in NTP multicast server mode, it multicasts a clock synchronization packet periodically. The devices which are configured to be in the

NTP multicast client mode will respond this packet and start the clock synchronization procedure. In this mode, the switch can accommodate up to 1,024 multicast clients.



- *The total number of the servers and peers configured for a switch can be up to 128.*
- *After the configuration, the Switch 7750 does not establish connections with the peer if it operates in NTP server mode. Whereas if it operates in any of the other modes, it establishes connections with the peer.*
- *If a Switch 7750 operates as a passive peer in peer mode, NTP broadcast client mode, or NTP multicast client mode, the connections it establishes with the peers are dynamic. If it operates in other modes, the connections it establishes with the peers are static.*

Access Control Permission Configuration

Access control permission to NTP server is a security measure that is of the minimum extent. Authentication is more reliable comparing to it.

An access request made to an NTP server is matched from the highest permission to the lowest, that is, in the order of **peer**, **server**, **synchronization**, and **query**.

Table 603 Configure the access control permission to the local NTP server

Operation	Command	Description
Enter system view	**system-view**	-
Configure the access control permission to the local NTP server	**ntp-service access** { **peer** | **server** | **synchronization** | **query** } *acl-number*	Optional By default, the access control permission to the local NTP server is **peer**

NTP Authentication Configuration

For the networks with higher security requirements, you can specify to perform authentications when enabling NTP. With the authentications performed on both the client side and the server side, the client is synchronized only to the server that passes the authentication. This improves network security.

Prerequisites

NTP authentication configuration involves:

- Configuring NTP authentication on the client
- Configuring NTP authentication on the server

Note the following when performing NTP authentication configuration:

- If the NTP authentication is not enabled on a client, the client can be synchronized to a server regardless of the NTP authentication configuration performed on the server (assuming that the related configurations are performed).
- You need to couple the NTP authentication with a trusted key.
- The configurations performed on the server and the client must be the same.
- A client with NTP authentication enabled is only synchronized to a server that can provide a trusted key.

Configuring NTP Authentication

Configuring NTP authentication on the client

Table 604 Configure NTP authentication on the client

Operation	Command	Description
Enter system view	**system-view**	-
Enable NTP authentication globally	**ntp-service authentication enable**	Required By default, the NTP authentication is disabled
Configure the NTP authentication key	**ntp-service authentication-keyid** *key-id* **authentication-model md5** *value*	Required By default, the NTP authentication key is not configured
Configure the specified key to be a trusted key	**ntp-service reliable authentication-keyid** *key-id*	Required By default, no trusted authentication key is configured
Associate the specified key with the corresponding NTP server	NTP client mode: **ntp-service unicast-server** { *remote-ip* | *server-name* } **authentication-keyid** *key-id* Peer mode: **ntp-service unicast-peer** { *remote-ip* | *peer-name* } **authentication-keyid** *key-id*	■ In NTP client mode and NTP peer mode, you need to associate the specified key with the corresponding NTP server on the client. ■ You can associate the NTP server with the authentication key while configuring the switch to operate in a specific NTP mode. You can also associate them using this command after configuring the NTP mode where the switch is to operate



- *NTP authentication requires that the authentication keys configured for the server and the client are the same. Besides, the authentication keys must be trusted keys. Otherwise, the client cannot be synchronized with the server.*
- *In NTP server mode and NTP peer mode, you need to associate the specified key with the corresponding NTP server/active peer on the client/passive peer. In these two modes, multiple servers/active peers may be configured for a client/passive peer, and a client/passive choose the server/active peer to synchronize to by the authentication key.*

Configuring NTP authentication on the server

Table 605 Configure NTP authentication on the server

Operation	Command	Description
Enter system view	**system-view**	-
Enable NTP authentication	**ntp-service authentication enable**	Required By default, NTP authentication is disabled
Configure NTP authentication key	**ntp-service authentication-keyid** *key-id* **authentication-model md5** *value*	Required By default, NTP authentication key is not configured

Table 605 Configure NTP authentication on the server

Operation	Command	Description
Configure the specified key to be a trusted key	**ntp-service reliable authentication-keyid** *key-id*	Required By default, an authentication key is not a trusted key
Enter VLAN interface view	**interface** *interface-type interface-number*	-
Associate a specified key with the corresponding NTP server	Broadcast server mode: **ntp-service broadcast-server authentication-keyid** *key-id* Multicast server mode: **ntp-service multicast-server authentication-keyid** *key-id*	■ In NTP broadcast server mode and NTP multicast server mode, you need to associate the specified key with the corresponding NTP server on the server ■ You can associate an NTP server with an authentication key while configuring a switch to operate in a specific NTP mode. You can also associate them using this command after configuring the NTP mode where a switch is to operate

The procedures for configuring NTP authentication on the server are the same as that on the client. Besides, the client and the server must be configured with the same authentication key.

Configuration of Optional NTP Parameters

The configurations of optional NTP parameters are:

- Setting the local clock as the NTP master clock
- Configuring the local VLAN interface that sends NTP packets
- Configuring the number of the dynamic sessions that can be established locally
- Disabling the VLAN interface configured on a switch from receiving NTP packets
- Disabling NTP service globally

Table 606 Configure optional NTP parameters

Operation	Command	Description
Enter system view	**system-view**	-
Configure the local clock as the NTP master clock	**ntp-service refclock-master** [*ip-address*] [*stratum*]	Optional
Configure the local interface that sends NTP packets	**ntp-service source-interface** *interface-type interface-number*	Optional
Configure the number of the sessions that can be established locally	**ntp-service max-dynamic-sessions** *number*	Optional By default, up to 100 dynamic sessions can be established locally.
Enter VLAN interface view	**interface** *interface-type interface-number*	-

Table 606 Configure optional NTP parameters

Operation	Command	Description
Disable the interface from receiving NTP packets	**ntp-service in-interface disable**	Optional By default, a VLAN interface receives NTP packets.
Return to system view	**quit**	-
Disable NTP service globally	**ntp-service disable**	Optional By default, the NTP service is enabled



CAUTION:

- *The source IP address in an NTP packet is the address of the sending interface specified by the ntp-service unicast-server command or the ntp-service unicast-peer command if you provide the address of the sending interface in these two commands.*
- *Dynamic connections can only be established when a switch operates in passive peer mode, NTP broadcast client mode, or NTP multicast client mode. In other modes, the connections established are static.*

Displaying and Debugging NTP

After the above configuration, you can execute the **display** command in any view to display the running status of the NTP configuration, and verify the effect of the configuration.

Table 607 Display and debug NTP

Operation	Command	Description
Display the status of NTP service	**display ntp-service status**	The **display** command can be executed in any view
Display the information about the sessions maintained by NTP	**display ntp-service sessions** [**verbose**]	
Display the brief information about the NTP time servers of the reference clock sources that the local device traces to	**display ntp-service trace**	

Configuration Example

NTP Server Mode Configuration

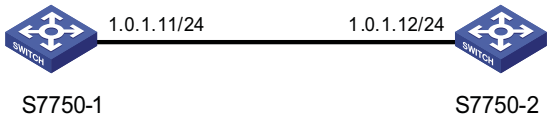
Network requirements

Configure the local clock of S7750-1 to be the NTP master clock, with the stratum being 2.

S7750-2 operates in client mode, with S7750-1 as the time server. S7750-1 operates in server mode automatically.

Network diagram

Figure 197 Network diagram for the NTP server mode configuration



Configuration procedures

Configure S7750-1.

Set the local clock as the NTP master clock, with the stratum being 2.

```
<SW7750-1> system-view
System View: return to User View with Ctrl+Z.
[SW7750-1] ntp-service refclock-master 127.127.1.1 2 ?
```

The following configurations are for S7750-2.

View the NTP status of S7750-2 before synchronization.

```
<SW7750-2> display ntp-service status
Service status: enabled
Clock status: unsynchronized
Clock stratum: 16
Reference clock ID: none
Nominal frequence: 99.8562 Hz
Actual frequence: 99.8562 Hz
Clock precision: 2^7
Clock offset: 0.0000 ms
Root delay: 0.00 ms
Root dispersion: 0.00 ms
Peer dispersion: 0.00 ms
Reference time: 00:00:00.000 UTC Jan 1 1900 (00000000.00000000)
```

Configure S7750-1 to be the time server of S7750-2.

```
<SW7750-2> system-view
[SW7750-2] ntp-service unicast-server 1.0.1.11
```

After the above configuration, S7750-2 is synchronized to S7750-1. View the NTP status of S7750-2.

```
[SW7750-2] display ntp-service status
Service status: enabled
Clock status: synchronized
Clock stratum: 3
Reference clock ID: 1.0.1.11
Nominal frequence: 250.0000 Hz
Actual frequence: 249.9992 Hz
Clock precision: 2^19
Clock offset: 0.66 ms
Root delay: 27.47 ms
Root dispersion: 208.39 ms
Peer dispersion: 9.63 ms
Reference time: 17:03:32.022 UTC Thu Sep 6 2001 (BF422AE4.05AEA86C)
```

The above output information indicates that S7750-2 is synchronized to S7750-1, and the stratum of its clock is 3, one stratum higher than S7750-1.

View the information about the NTP sessions of S7750-2. You can see that S7750-2 establishes a connection with S7750-1.

```
[SW7750-2]dis ntp-service sessions
     source        reference       stra reach poll  now offset  delay disper
**************************************************************************
    [12345]1.0.1.11     127.127.1.1         2    1   64    1   350.1   15.1   0.0
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
```

NTP Peer Mode Configuration

Network requirements

3Com2 sets the local clock to be the NTP master clock, with the clock stratum being 2.

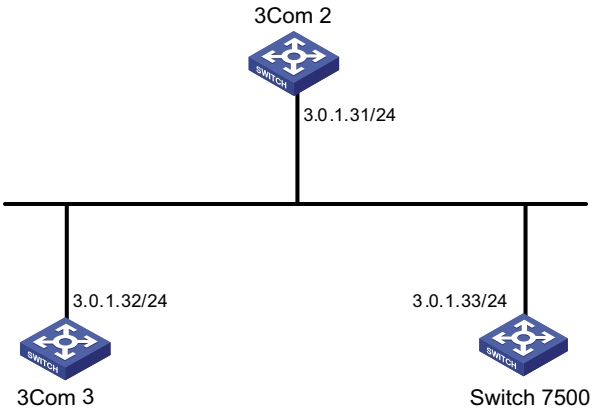
Configure a Switch 7750 to operate as a client, with 3Com2 as the time server. 3Com2 will then operate in the server mode automatically. Meanwhile, 3Com3 sets the Switch 7750 to be its peer.

This example assumes that

- *3Com2 is a switch that allows its local clock to be the master clock.*
- *3Com3 is a switch that allows its local clock to be the master clock and the stratum of its clock is 1.*

Network diagram

Figure 198 Network diagram for NTP peer mode configuration



Configuration procedures

1 Configure the Switch 7750.

Set 3Com2 to be the time server.

```
<SW7750> system-view
[SW7750] ntp-service unicast-server 3.0.1.31
```

2 Configure 3Com3 (after the Switch 7750 is synchronized to 3Com2).

Enter system view.

```
<SW77503> system-view
[SW77503]
```

After the local synchronization, set the Switch 7750 to be its peer.

```
[SW77503] ntp-service unicast-peer 3.0.1.32
```

The Switch 7750 and 3Com3 are configured to be peers with regard to each other. 3Com3 operates in the active peer mode, while the Switch 7750 operates in the passive peer mode. Because the stratum of the local clock of 3Com3 is 1, and that of the Switch 7750 is 3, the Switch 7750 is synchronized to Qudiway3.

View the status of the Switch 7750 after the synchronization.

```
[SW7750] display ntp-service status
Service status: enabled
Clock status: synchronized
 Clock stratum: 2
 Reference clock ID: 3.0.1.32
 Nominal frequency: 250.0000 Hz
 Actual frequency: 249.9992 Hz
 Clock precision: 2^19
Clock offset: 0.66 ms
 Root delay: 27.47 ms
 Root dispersion: 208.39 ms
 Peer dispersion: 9.63 ms
 Reference time: 17:03:32.022 UTC Thu Sep 6 2001 (BF422AE4.05AEA86C)
```

The output information indicates that the Switch 7750 is synchronized to 3Com3 and the stratum of its local clock is 2, one stratum higher than 3Com3.

View the information about the NTP sessions of the Switch 7750 and you can see that a connection is established between the Switch 7750 and 3Com3.

```
[SW7750] display ntp-service sessions
     source        reference       stra reach poll  now offset  delay disper
**************************************************************************
[2]3.0.1.32         127.127.1.0        1    1   64    1  350.1   15.1    0.0
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
```

NTP Broadcast Mode Configuration

Network requirements

3Com3 sets its local clock to be an NTP master clock, with the stratum being 2. NTP packets are broadcast through VLAN interface 2.

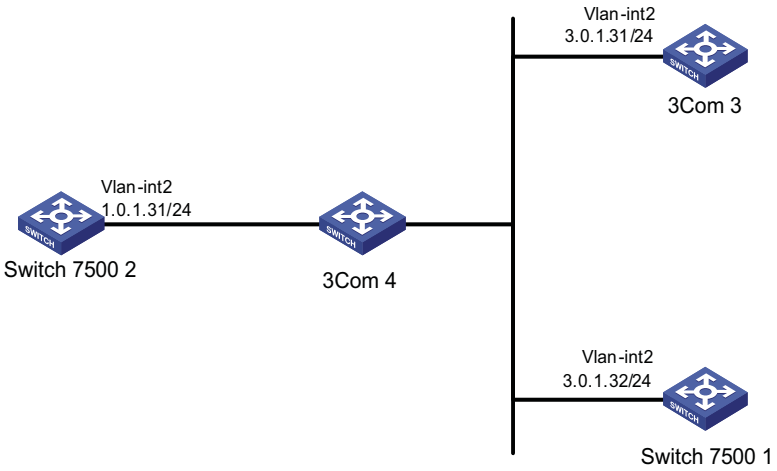
Configure S7750-1 and S7750-2 to listen to broadcast packets through their VLAN interface 2.



This example assumes that 3Com3 is a switch that supports the local clock being the master clock.

Network diagram

Figure 199 Network diagram for the NTP broadcast mode configuration



Configuration procedures

1 Configure 3Com3.

Enter system view.

```
<SW77503> system-view
[SW77503]
```

Enter VLAN-interface 2 view.

```
[SW77503] interface Vlan-interface 2
[SW77503-Vlan-Interface2]
```

Configure 3Com3 to be the broadcast server and send broadcast packets through VLAN-interface 2.

```
[SW77503-Vlan-Interface2] ntp-service broadcast-server
```

2 Configure Switch 7750-1.

Enter system view.

```
<SW7750-1> system-view
[SW7750-1]
```

Enter VLAN-interface 2 view.

```
[SW7750-1] interface Vlan-interface 2
[SW7750-1-Vlan-Interface2]
```

Configure Switch 7750-1 to be a broadcast client.

```
[SW7750-1-Vlan-Interface2] ntp-service broadcast-client
```

3 Configure Switch 7750-2

Enter system view.

```
<SW7750-2> system-view
[s7500-2]
```

Enter VLAN-interface 2 view.

```
[SW7750-2] interface Vlan-interface 2
[SW7750-2-Vlan-Interface2]
```

Configure Switch 7750-2 to be a broadcast client.

```
[SW7750-2-Vlan-interface2] ntp-service broadcast-client
```

The above configuration configures Switch 7750-1 and Switch 7750-2 to listen to broadcast packets through their VLAN interface 2, and 3Com3 to send broadcast packets through VLAN interface 2. Because Switch 7750-2 does not reside in the same network segment with 3Com3, Switch 7750-2 cannot receive broadcast packets sent by 3Com3, while Switch 7750-1 is synchronized to 3Com3 after receiving broadcast packets sent by 3Com3.

View the status of Switch 7750-1 after the synchronization.

```
[SW7750-1] display ntp-service status
Service status: enabled
Clock status: synchronized
 Clock stratum: 3
 Reference clock ID: 3.0.1.31
 Nominal frequency: 250.0000 Hz
 Actual frequency: 249.9992 Hz
 Clock precision: 2^19
 Clock offset: 198.7425 ms
 Root delay: 27.47 ms
 Root dispersion: 208.39 ms
 Peer dispersion: 9.63 ms
 Reference time: 17:03:32.022 UTC Thu Sep 6 2001 (BF422AE4.05AEA86C)
```

The output information indicates that Switch 7750-1 is synchronized to 3Com3, with the clock stratum of 3, one stratum higher than 3Com3.

View the information about the NTP sessions of Switch 7750-1 and you can see that a connection is established between Switch 7750-1 and 3Com3.

```
[SW7750-1] display ntp-service sessions
    source          reference       stra reach poll  now offset   delay disper
**************************************************************************
[1]3.0.1.31        127.127.1.0      2    1    64   377    26.1   199.53   9.7
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
```

NTP Multicast Mode Configuration

Network requirements

3Com3 sets the local clock to be NTP master clock, with the clock stratum of 2. It advertises multicast packets through VLAN interface 2.

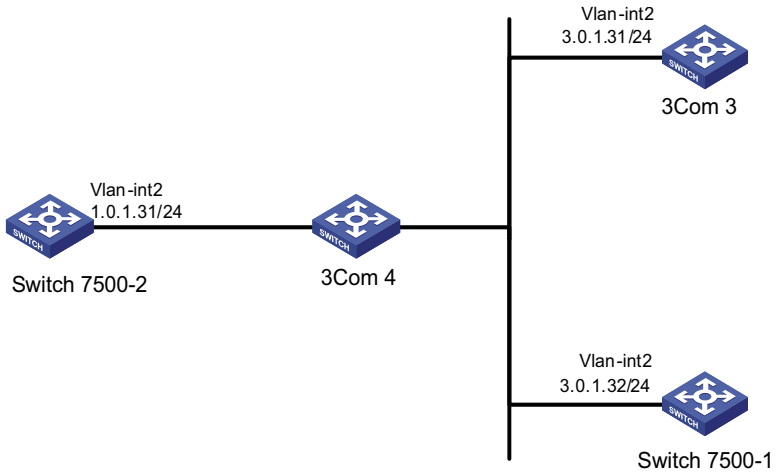
Configure Switch 7750-1 and Switch 7750-2 to listen to multicast packets through their VLAN interface 2.



This example assumes that 3Com3 is a switch that supports the local clock being the master clock.

Network diagram

Figure 200 Network diagram for NTP multicast mode configuration



Configuration procedures

1 Configure 3Com3.

Enter system view.

```
<SW77503> system-view
[SW77503]
```

Enter VLAN-interface 2 view.

```
[SW77503] interface Vlan-interface 2
```

Configure 3Com3 to be a multicast server.

```
[SW77503-Vlan-Interface2] ntp-service multicast-server
```

2 Configure Switch 7750-1.

Enter system view.

```
<SW7750-1> system-view
[SW7750-1]
```

Enter VLAN-interface 2 view.

```
[[SW7750-1] interface vlan-interface 2
```

Configure 3Com4 to be a multicast client.

```
[SW7750-1-Vlan-interface2] ntp-service multicast-client
```

3 Configure Switch 7750-2.

Enter system view.

```
<SW7750-2> system-view
[SW7750-2]
```

Enter VLAN-interface 2 view.

```
[[SW7750-2] interface Vlan-interface 2
```

Configure Switch 7750-2 to be a multicast client.

```
[SW7750-2-Vlan-Interface2] ntp-service multicast-client
```

The above configuration configures Switch 7750-1 and Switch 7750-2 to listen to multicast packets through their VLAN interface 2, and 3Com3 to advertise multicast packets through VLAN interface 2. Because Switch 7750-2 does not reside in the same network segment with 3Com3, Switch 7750-2 cannot receive multicast packets sent by 3Com3, while Switch 7750-1 is synchronized to 3Com3 after receiving multicast packets sent by 3Com3.

View the status of Switch 7750-1 after the synchronization.

```
[SW7750-1] display ntp-service status
Service status: enabled
Clock status: synchronized
 Clock stratum: 3
 Reference clock ID: 3.0.1.31
 Nominal frequency: 250.0000 Hz
 Actual frequency: 249.9992 Hz
 Clock precision: 2^19
 Clock offset: 198.7425 ms
 Root delay: 27.47 ms
 Root dispersion: 208.39 ms
 Peer dispersion: 9.63 ms
 Reference time: 17:03:32.022 UTC Thu Sep 6 2001 (BF422AE4.05AEA86C)
```

The output information indicates that Switch 7750-1 is synchronized to 3Com3, with the clock stratum being 3, one stratum higher than 3Com3.

View the information about the NTP sessions of Switch 7750-1 and you can see that a connection is established between Switch 7750-1 and 3Com3.

```
[SW7750-1] display ntp-service sessions
    source          reference       stra reach poll  now offset  delay disper
**************************************************************************
[1]3.0.1.31        127.127.1.0      2    1    64   377    26.1   199.53   9.7
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
```

NTP Server Mode with Authentication Configuration

Network requirements

The local clock of Switch 7750-1 operates as the master NTP clock, with the clock stratum being 2.

Switch 7750-2 operates in client mode with Switch 7750-1 as the time server. Switch 7750-1 operates in the server mode automatically. Meanwhile, NTP authentication is enabled on both sides.

Network diagram

Figure 201 Network diagram for NTP server mode with authentication configuration



Configuration procedures

1 Configure Switch 7750-2.

Enter system view.

```
<SW7750-2 > system-view
[SW7750-2]
```

Configure Switch 7750-1 to be the time server.

```
[SW7750-2] ntp-service unicast-server 1.0.1.11
```

Enable NTP authentication.

```
[SW7750-2] ntp-service authentication enable
```

Set the MD5 key to 42, with the content being aNiceKey.

```
[SW7750-2] ntp-service authentication-keyid 42 authentication-mode m
d5 aNiceKey
```

Specify the key to be a trusted key.

```
[SW7750-2] ntp-service reliable authentication-keyid 42
[[SW7750-2] ntp-service unicast-server 1.0.1.11 authentication-keyid 42
```

The above configuration synchronizes Switch 7750-2 to Switch 7750-1. As NTP authentication is not enabled on Switch 7750-1, Switch 7750-2 will fail to be synchronized to Switch 7750-1.

The following configuration is needed for Switch 7750-1.

Enable authentication on 3Com1.

```
[SW7750-1] system-view
[SW7750-1] ntp-service authentication enable
```

Set the MD5 key to 42, with the content being aNiceKey.

```
[SW7750-1] ntp-service authentication-keyid 42 authentication-model
md5 aNiceKey
```

Specify the key to be a trusted key.

```
[SW7750-1] ntp-service reliable authentication-keyid 42
```

After the above configuration, Switch 7750-2 can be synchronized to Switch 7750-1. You can view the status of Switch 7750-2 after the synchronization.

```
[SW7750-2] display ntp-service status
Service status: enabled
Clock status: synchronized
Clock stratum: 3
Reference clock ID: 1.0.1.11
Nominal frequence: 250.0000 Hz
Actual frequence: 249.9992 Hz
Clock precision: 2^19
Clock offset: 0.66 ms
Root delay: 27.47 ms
Root dispersion: 208.39 ms
Peer dispersion: 9.63 ms
Reference time: 17:03:32.022 UTC Thu Sep 6 2001 (BF422AE4.05AEA86C)
```

The output information indicates that Switch 7750-2 is synchronized to Switch 7750-1, with the clock stratum being 3, one stratum higher than Switch 7750-1.

View the information about the NTP sessions of Switch 7750-2 and you can see that a connection is established between Switch 7750-2 and Switch 7750-1.

```
<SW7750-2> display ntp-service sessions
     source        reference       stra reach poll  now offset  delay disper
**************************************************************************
    [5]1.0.1.11    127.127.1.0    2    1      64    1   350.1   15.1    0.0
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
```

71 SSH TERMINAL SERVICES

SSH Terminal Services

Introduction to SSH

Secure Shell (SSH) can provide information security and powerful authentication to prevent such attacks as IP address spoofing, plain-text password interception when users log on to the Switch remotely through an insecure network.

As an SSH server, a switch can connect to multiple SSH clients; as an SSH client, a switch can establish SSH connections with switches or UNIX hosts that support SSH server.

Currently, the Switch 7750 supports SSH2.0 (compatible with SSH1.5).

The communication process between the server and client includes these five stages:

1 Version negotiation stage. These operations are completed at this stage:

- The client sends TCP connection requirement to the server.
- When TCP connection is established, both ends begin to negotiate the SSH version.
- If they can work together in harmony, they enter the key algorithm negotiation stage. Otherwise the server clears the TCP connection.

2 Key algorithm negotiation stage. These operations are completed at this stage:

- The server and the client send key algorithm negotiation packets to each other, which include the supported public key algorithm list, encryption algorithm list, MAC algorithm list, and compression algorithm list.
- Based on the received algorithm negotiation packets, the server and the client figure out the algorithms to be used.
- The server and the client use the DH key exchange algorithm and parameters such as the host key pair to generate the session key and session ID.

Through the above steps, the server and the client get the same session key, which is to be used to encrypt and decrypt data exchanged between the server and the client later. The server and the client use session ID in the authentication stage.

3 Authentication method negotiation stage.

The client sends an authentication request carrying the username and authentication method to the server. The server starts to authenticate the user.

SSH supports two authentication types: password authentication and RSA authentication.

- Password authentication works as follows: The client sends a password authentication request carrying the encrypted username and password to the server. The server decrypts the request to obtain the username and password in plain text, and matches the username and password against those configured on itself. Then, it returns the authentication result according to the matching result.
- RSA authentication works as follows: The client sends an RSA authentication request carrying the username, public key and public key algorithm to the server. The server checks the validity of the public key. If the key is invalid, the server returns an authentication failure message directly; otherwise, the server authenticates the client and returns the authentication result to the client.

4 Session request stage. After successful authentication, the client sends session request messages to the server. The server processes the request messages.

5 Interactive session stage. Both ends exchange data till the session ends.

SSH Server Configuration

The following table describes SSH server configuration tasks.

Table 608 Configure SSH2.0 server

Configuration	Keyword	Description
Configure supported protocols	**protocol inbound**	Refer to "Configuring supported protocols" on page 774
Generate a local RSA key pair	**rsa local-key-pair create**	Refer to "Generating or destroying RSA key pairs" on page 775
Destroy a local RSA key pair	**rsa local-key-pair destroy**	
Create an SSH user	**ssh user** *username*	Refer to "Creating an SSH user" on page 776.
Specify a default authentication type for SSH users	**ssh authentication-type default**	Refer to "Configuring authentication type" on page 776
Configure authentication type for SSH users	**ssh user** *username* **authentication-type**	
Set SSH authentication timeout time	**ssh server timeout**	Refer to "Configuring server SSH attributes" on page 777
Set SSH authentication retry times	**ssh server authentication-retries**	
Set the update interval for the server key	**ssh server rekey-interval**	
Specify the server compatible with the SSH1.x version-supported client.	**ssh server compatible-ssh1x enable**	
Allocate public keys for SSH users	**ssh user** *username* **assign rsa-key** *keyname*	Refer to "Configuring a Client Public Key" on page 777

Configuring supported protocols

Table 609 Configure supported protocols

Operation	Command	Description
Enter system view	**system-view**	-

Table 609 Configure supported protocols

Operation	Command	Description
Enter one or multiple user interface views	**user-interface** [*type-keyword*] *number* [*ending-number*]	Required
Configure the protocols supported in the user interface view(s)	**protocol inbound** { **all** |**ssh** | **telnet** }	Optional By default, the system supports both Telnet and SSH

CAUTION:

- *When SSH protocol is specified, to ensure a successful login, you must configure the AAA authentication using the* ***authentication-mode scheme*** *command.*
- *The* ***protocol inbound ssh*** *configuration fails if you configured* ***authentication-mode password*** *or* ***authentication-mode none****. When you configure SSH protocol successfully for the user interface, then you cannot configure* ***authentication-mode password*** *or* ***authentication-mode none*** *any more.*

Generating or destroying RSA key pairs

This configuration task is used to generate or destroy the server RSA key pair, including the host RSA key pair and the server RSA key pair.

- The name of the host RSA key pair is in the format of switch name plus _Host, for example, 3Com_Host.
- The name of the server RSA key pair is in the format of switch name plus _Server, for example, 3Com_Server.

Server RSA key pair (3Com_Server) is not used in SSH2.0; therefore, when the ***rsa local-key-pair create*** *command is executed, the system only prompts you the host RSA key pair (3Com_Host) is generated, and does not inform you the information about the server RSA key pair even if the server RSA key pair is generated in the background for the purpose of SSH1.x compatibility. You can use the* ***display rsa local-key-pair public*** *command to display the generated key pairs.*

After you configure the **rsa local-key-pair** command, the system prompts you to define the key length.

- In SSH1.x, the key length is in the range of 512 to 2,048 (bits).
- In SSH2.0, the key length is in the range of 768 to 2,048 (bits).

Table 610 Generate or destroy RSA key pairs

Operation	Command	Description
Enter system view	**system-view**	-
Generate a local RSA key pair	**rsa local-key-pair create**	Required
Destroy a local RSA key pair	**rsa local-key-pair destroy**	Optional

CAUTION:

- *For a successful SSH login, you must generate a local RSA key pair first.*

- *You just need to execute the command once, with no further action required even after the system is rebooted.*
- *If you use this command to generate an RSA key provided an old one exits, the system will prompt you whether to replace the previous one or not.*

Creating an SSH user

This configuration task is used to configure an SSH user.

Table 611 Create an SSH user

Operation	Command	Description
Enter system view	**system-view**	-
Create an SSH user	**ssh user** *username*	Optional

Note that: an SSH user created in this way adopts the default authentication type if you do not use the **ssh user authentication-type** command to specify an authentication type for this user.

Configuring authentication type

New users must specify authentication type. Otherwise, they cannot access the switch.

Table 612 Configure authentication type

Operation	Command	Description
Enter system view	**system-view**	-
Specify a default authentication type for SSH users	**ssh authentication-type default** { **password** | **rsa** | **password-publickey** | **all** }	Optional; By default, the password authentication type is specified.
Configure authentication type for SSH users	**ssh user** *username* **authentication-type** { **password** | **rsa** | **password-publickey** | **all** }	Optional By default, the system does not specify available authentication types for SSH users, that is, they cannot access the switch

Note that:

- Use the **ssh authentication-type default** command to configure the default authentication type for all users.
- Use **the ssh user** *username* **authentication-type** command to specify the authentication type for a user.
- When the two commands are configured simultaneously, and the authentication types configured for the user (specified by *username*) are different with each other, comply with the configuration of the **ssh user** *username* **authentication-type** command.



CAUTION:

- *If RSA authentication type is defined, then the RSA public key of the client user must be configured on the switch.*

- *For the **password-publickey** authentication type: SSH1 client users can access the switch as long as they pass one of the two authentications. SSH2.0 client users can access the switch only when they pass both the authentications.*
- *For the **password** authentication, username should be consistent with the effective username defined in AAA; for the RSA authentication, username is the SSH local username, so that there is no need to configure a local user in AAA.*

Configuring server SSH attributes

Configuring server SSH authentication timeout time, retry times, server keys update interval and SSH compatible mode can effectively assure security of SSH connections by avoiding illegal actions such as malicious password guessing.

Table 613 Configure server SSH attributes

Operation	Command	Description
Enter system view	**system-view**	-
Set SSH authentication timeout time	**ssh server timeout** *seconds*	Optional The timeout time defaults to 60 seconds.
Set SSH authentication retry times	**ssh server authentication-retries** *times*	Optional The retry times defaults to 3.
Set server keys update interval	**ssh server rekey-interval**	Optional By default, the system does not update server keys.
Set SSH server compatible with SSH1.x client	**ssh server compatible-ssh1x enable**	Optional By default, SSH server is compatible with SSH1.x client.

Configuring a Client Public Key

You can configure RSA public keys for client users on the switch and specify RSA private keys, which correspond to the public keys, on the client. The client public keys are generated randomly by the SSH2.0 client. This operation is not required for password authentication type.

On the other hand, you can import the RSA public key of an SSH user from the public key file. When the **rsa peer-public-key** *keyname* **import sshkey** *filename* command is executed, the system will transform the format of the public key file created on the client into the public key cryptography standards (PKCS) format and configure the client public key automatically. Before the configuration above, the client must upload the public key file of the RSA key to the server by using FTP/TFTP.

Table 614 Configure client public keys

Operation	Command	Description
Enter system view	**system-view**	-
Enter public key view	**rsa peer-public-key** *key-name*	Required

Table 614 Configure client public keys

Operation	Command	Description
Enter public key edit view	**public-key-code begin**	You can key in a blank space between characters, since the system can remove the blank space automatically. But the public key should be composed of hexadecimal characters.
Return to public key view from public key edit view	**public-key-code end**	The system saves public key data when exiting from public key edit view
Return to system view from public key view	**peer-public-key end**	-
Allocate public keys to SSH users	**ssh user** *username* **assign rsa-key** *keyname*	Required *Keyname* is the name of an existing public key. If the user already has a public key, the new public key overrides the old one.

Table 615 Import the RSA public key of an SSH user from the public key file

Operation	Command	Description
Enter system view	**system-view**	-
Import the RSA public key of an SSH user from the public key file	**rsa peer-public-key** *keyname* **import sshkey** *filename*	Required

SSH Client Configuration

Configuration prerequisites

Make sure that the SSH server is configured. Refer to "SSH Server Configuration" on page 774 for configuration details.

Configure the device as an SSH client

When a device operating as an SSH client connects to the server, you can specify whether the SSH client performs first-time authentication for the SSH server to be accessed.

- With first-time authentication enabled, when the SSH client accesses the SSH server for the first time, the user can continue to access the SSH server and the host public key will be saved on the client even if the server host public key is not configured on the client. When the SSH client accesses the SSH server next time, the SSH client uses the host public key saved on it to authenticate the SSH server.
- With first-time authentication disabled, the SSH client cannot access the SSH server if the server host public key is not configured on the client. Before configuring a device as an SSH client, you need to configure the host public key of the server to be accessed on the local device and specify the name of the host public key file of the server to be accessed. Thus, the SSH client can authenticate the SSH server to be accessed.

Table 616 Configure a device as an SSH client

Operation	Command	Description
Enter system view	**system-view**	-
Disable the SSH client from performing first-time authentication for the SSH server to be accessed	**undo ssh client first-time**	Optional By default, the SSH client performs first-time authentication.
Configure the public key of the server on the client	Refer to "Configuring a Client Public Key" on page 777	Required if first-time authentication is not configured on the client The method of configuring a server public key on the client is the same as that of configuring a client public key on the server.
Specify the name of the host public key of the SSH server to be accessed on the SSH client	**ssh client** *server-ip* **assign rsa-key** *keyname*	Required if first-time authentication is not configured on the client
Connect the SSH client to the SSH server, and specify the preferred key exchange algorithm, the preferred encryption algorithm and the preferred HMAC algorithm for the SSH client and the SSH server	**ssh2** { *host-ip* | *host-name* } [*port-number*] [**prefer_kex** { **dh_group1** | **dh_exchange_group** } | **prefer_ctos_cipher** { **des** | **aes128**} | **prefer_stoc_cipher** { **des** | **aes128** } | **prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** } | **prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }]*	Required

Displaying SSH Configuration

Use the **display** commands in any view to view the running of SSH and further to check the configuration result. Through the displaying information, you can verify the configuration effect.

Table 617 Display SSH configuration

Operation	Command	Description
Display host and server public keys	**display rsa local-key-pair public**	**display** command can be executed in any view
Display information about the peer public keys	**display rsa peer-public-key** [**brief** | **name** *keyname*]	
Display SSH status and session information	**display ssh server** { **status** | **session** }	
Display SSH user information	**display ssh user-information** [*username*]	
Display the mappings between host public keys and SSH servers saved on a client	**display ssh server-info**	

SSH Server Configuration Example

Network requirements

As shown in Figure 202, The PC (SSH Client) runs the client software which supports SSH2.0, establish a local connection with the switch (SSH Server) and ensure the security of data exchange.

Network diagram

Figure 202 Network diagram for SSH server configuration



Configuration procedure

1 Generate a local RSA key pair.

```
<SW7750> system-view
[SW7750] rsa local-key-pair create
```

If the local RSA key pair has been generated in previous operations, skip this step here.

2 Set authentication type.

Settings for the two authentication types are described respectively in the following:

- Password authentication

Set AAA authentication on the user interfaces.

```
[SW7750] user-interface vty 0 4
[SW7750-ui-vty0-4] authentication-mode scheme
```

Set the user interfaces to support SSH.

```
[SW7750-ui-vty0-4] protocol inbound ssh
```

Configure the login protocol for user clinet001 as SSH and authentication type as password.

```
[SW7750] local-user client001
[SW7750-luser-client001] password simple abc
[SW7750-luser-client001] service-type ssh
[SW7750-luser-client001] quit
[SW7750] ssh user client001 authentication-type password
```

Select the default SSH authentication timeout time and authentication retry times. After these settings, run the SSH2.0-supported client software on other hosts connected to the switch. Log in to the switch using username client001 and password abc.

- RSA public key authentication

Set AAA authentication on the user interfaces.

```
[SW7750] user-interface vty 0 4
[SW7750-ui-vty0-4] authentication-mode scheme
```

Set the user interfaces to support SSH.

```
[SW7750-ui-vty0-4] protocol inbound ssh
```

Configure the login protocol for user client002 as SSH and authentication type as RSA public key.

```
[SW7750] ssh user client002 authentication-type rsa
```

Generate randomly RSA key pairs on the SSH2.0 client and send the corresponding public keys to the server.

Configure client public keys on the server, with their name as 3Com002.

```
[SW7750] rsa peer-public-key 3Com002
[SW7750-rsa-public-key] public-key-code begin
[SW7750-rsa-key-code] 308186028180739A291ABDA704F5D93DC8FDF84C427463
[SW7750-rsa-key-code] 1991C164B0DF178C55FA833591C7D47D5381D09CE82913
[SW7750-rsa-key-code] D7EDF9C08511D83CA4ED2B30B809808EB0D1F52D045DE4
[SW7750-rsa-key-code] 0861B74A0E135523CCD74CAC61F8E58C452B2F3F2DA0DC
[SW7750-rsa-key-code] C48E3306367FE187BDD944018B3B69F3CBB0A573202C16
[SW7750-rsa-key-code] BB2FC1ACF3EC8F828D55A36F1CDDC4BB45504F020125
[SW7750-rsa-key-code] public-key-code end
[SW7750-rsa-public-key] peer-public-key end
[SW7750] ssh user client002 assign rsa-key 3Com002
```

Start the SSH client software on the host which stores the RSA private keys and make corresponding configuration to establish an SSH connection.

SSH Client Configuration Example

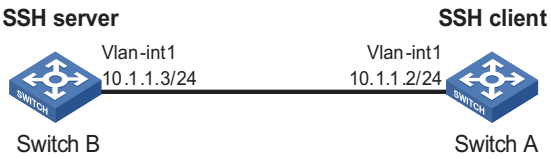
Network requirements

As shown in Figure 203,

- Switch A serves as an SSH client and uses the username of client001 and IP address of 10.1.1.2/24.
- Switch B serves as an SSH server, with its IP address 10.1.1.3/24.
- RSA authentication method is adopted to enhance the security.
- The SSH client authenticates the SSH server to ensure the validity of the SSH server.

Network diagram

Figure 203 Network diagram for SSH client configuration



Configuration procedure

1 Configure Switch B (SSH server)

Create a VLAN interface on the switch and assign it an IP address, which the SSH client will use as the destination for SSH connection.

```
<SW7750> system-view
[SW7750] interface vlan-interface 1
```

```
[SW7750-Vlan-interface1] ip address 10.1.1.3 255.255.255.0
[SW7750-Vlan-interface1] quit
```



CAUTION: *Generating server RSA key pair is a must for SSH login.*

Generate an RSA key pair.

```
[SW7750] rsa local-key-pair create
```

Set the authentication mode for the user interfaces to AAA.

```
[SW7750] user-interface vty 0 4
[SW7750-ui-vty0-4] authentication-mode scheme
```

Enable the user interfaces to support SSH.

```
[SW7750-ui-vty0-4] protocol inbound ssh
```

Set the user command privilege level to 3.

```
[SW7750-ui-vty0-4] user privilege level 3
[SW7750-ui-vty0-4] quit
```

Create a user named client001, specifying to use RSA authentication.

```
[SW7750] ssh user client001 authentication-type rsa
```



Before performing the following tasks, you must generate an RSA key pair on the client, and configure the public key on the SSH server. For details, refer to "SSH Client Configuration" on page 778.

Configure the client public key on the server, and name the public key Switch001.

```
[SW7750] rsa peer-public-key Switch001
RSA public key view: return to System View with "peer-public-key end".
[SW7750-rsa-public-key] public-key-code begin
RSA key code view: return to last view with "public-key-code end".
[SW7750-rsa-key-code] 3047
[SW7750-rsa-key-code] 0240
[SW7750-rsa-key-code] C8969B5A 132440F4 0BDB4E5E 40308747 804F608B
[SW7750-rsa-key-code] 349EBD6A B0C75CDF 8B84DBE7 D5E2C4F8 AED72834
[SW7750-rsa-key-code] 74D3404A 0B14363D D709CC63 68C8CE00 57C0EE6B
[SW7750-rsa-key-code] 074C0CA9
[SW7750-rsa-key-code] 0203
[SW7750-rsa-key-code] 010001
[SW7750-rsa-key-code] public-key-code end
[SW7750-rsa-public-key] peer-public-key end
[SW7750]
```

Assign public key Switch001 to user client001.

```
[SW7750] ssh user client001 assign rsa-key Switch001
```



If the first-time authentication is not configured, it is required to manually configure the RSA host public key of the server on the client.

Display the RSA pubic key of the server (only the host public key contents are displayed).

```
[SW7750] display rsa local-key-pair public
=====================================================
Time of Key pair created: 09:04:41  2000/04/04
Key name: 3Com_Host
Key type: RSA encryption Key
=====================================================
Key code:
308188
  028180
    C9330FFD 2E2A606F 3BFD5554 8DACDFB8 4D754E86
    FC2D15E8 1996422A 0F6A2A6A A94A207E 1E25F3F9
    E0EA01A2 4E0F2FF7 B1D31505 39F02333 E443EE74
    5C3615C3 E5B3DC91 D41900F0 2AE8B301 E55B1420
    024ECF2C 28A6A454 C27449E0 46EB1EAF 8A918D33
    BAF53AF3 63B1FB17 F01E4933 00BE2EEA A272CD78
    C289B7DD 2BE0F7AD
  0203
    010001
```

<Omitted>

- Configure Switch A (SSH client)

Create a VLAN interface on the switch and assign it an IP address, which the SSH server will use as the destination for SSH connection.

```
<SW7750> system-view
[SW7750] interface vlan-interface 1
[SW7750-Vlan-interface1] ip address 10.1.1.2 255.255.255.0
[SW7750-Vlan-interface1] quit
```

Generate an RSA key pair.

```
[SW7750] rsa local-key-pair create
```

Display the RSA public key of the client (only the host public key contents are displayed).

```
<SW7750> display rsa local-key-pair public
=====================================================
Time of Key pair created: 05:15:04  2006/12/08
Key name: 3Com_Host
Key type: RSA encryption Key
=====================================================
Key code:
3047
  0240
    C8969B5A 132440F4 0BDB4E5E 40308747 804F608B
    349EBD6A B0C75CDF 8B84DBE7 D5E2C4F8 AED72834
    74D3404A 0B14363D D709CC63 68C8CE00 57C0EE6B
    074C0CA9
  0203
    010001
```

<Omitted>

After generating a key pair on a client, you need to configure the public key on the server and have the configuration on the server done before continuing configuration of the client.

Disable first-time authentication.

```
[SW7750] undo ssh client first-time
```

If the first-time authentication is not configured, it is required to manually configure the RSA host public key of the server on the client.

Configure the host public key of the server on the client, and name the public key Switch002.

```
[SW7750] rsa peer-public-key Switch002
RSA public key view: return to System View with "peer-public-key end".
[SW7750-rsa-public-key] public-key-code begin
RSA key code view: return to last view with "public-key-code end".
[SW7750-rsa-key-code] 308188
[SW7750-rsa-key-code] 028180
[SW7750-rsa-key-code] C9330FFD 2E2A606F 3BFD5554 8DACDFB8 4D754E86
[SW7750-rsa-key-code] FC2D15E8 1996422A 0F6A2A6A A94A207E 1E25F3F9
[SW7750-rsa-key-code] E0EA01A2 4E0F2FF7 B1D31505 39F02333 E443EE74
[SW7750-rsa-key-code] 5C3615C3 E5B3DC91 D41900F0 2AE8B301 E55B1420
[SW7750-rsa-key-code] 024ECF2C 28A6A454 C27449E0 46EB1EAF 8A918D33
[SW7750-rsa-key-code] BAF53AF3 63B1FB17 F01E4933 00BE2EEA A272CD78
[SW7750-rsa-key-code] C289B7DD 2BE0F7AD
[SW7750-rsa-key-code] 0203
[SW7750-rsa-key-code] 010001
[SW7750-rsa-key-code] public-key-code end
[SW7750-rsa-public-key] peer-public-key end
[SW7750]
```

Assign public key Switch002 to the server.

```
[SW7750] ssh client 10.1.1.3 assign rsa-key Switch002
```

Establish an SSH connection to the server 10.1.1.3.

```
[SW7750] ssh2 10.1.1.3
Username: client001
Trying 110.1.1.3 ...
Press CTRL+K to abort
Connected to 10.1.1.3 ...
***************************************************************
* Copyright (c) 2004-2007 Hangzhou 3Com Tech. Co., Ltd.       *
* Without the owner's prior written consent,                  *
* no decompiling or reverse-switch fabricering shall be allowed.  *
***************************************************************
<SW7750>
```

SFTP Service

SFTP Overview

Secure FTP (SFTP) is a new feature introduced in SSH2.0.

SFTP is established on SSH connections to secure remote users' login to the switch, perform file management and file transfer (such as upgrade the system), and

provide secured data transfer. As an SFTP client, it allows you to securely log onto another device to transfer files.

SFTP Server Configuration

The following sections describe SFTP server configuration tasks:

- "Configuring service type for an SSH user" on page 785
- "Enabling the SFTP server" on page 785

Configuring service type for an SSH user

Table 618 Configure service type for an SSH user

Operation	Command	Description
Enter system view	**system-view**	-
Configure service type for an SSH user	**ssh user** *username* **service-type** { **stelnet** | **sftp** | **all** }	Required By default, the available service type is **stelnet**.

*To support SFTP login, you need to set the service type to **sftp** or **all**.*

Enabling the SFTP server

Table 619 Enable the SFTP server

Operation	Command	Description
Enter system view	**system-view**	-
Enable the SFTP server	**sftp server enable**	Required By default, the SFTP server is not enabled.

SFTP Client Configuration

The following sections describe SFTP client configuration tasks:

Table 620 Configure SFTP client

Operation		Command Key word	View	Description
Enable the SFTP client		**sftp**	System view	Required
Disable the SFTP client		**bye**	SFTP client view	Optional
		exit		
		quit		
SFTP directory -related operations	Change the current directory	**cd**	SFTP client view	Optional
	Return to the upper directory	**cdup**		
	Display the current directory	**pwd**		
	Display the list of the files in a directory	**dir**		
		ls		
	Create a directory	**mkdir**		
	Delete a directory	**rmdir**		

Table 620 Configure SFTP client

Operation		Command Key word	View	Description
SFTP file-related operations	Rename a file or directory on the SFTP server	**rename**	SFTP client view	Optional
	Download a file from the remote SFTP server	**get**		
	Upload a local file to the remote SFTP server	**put**		
	Display the list of the files in a directory	**dir**		
		ls		
	Delete a file from the SFTP server	**delete**		
		remove		
Get help information about SFTP client commands		**help**	SFTP client view	Optional

Enabling the SFTP client

You can enable the SFTP client, establish a connection to the remote SFTP server and enter STP client view.

Table 621 Enable the SFTP client

Operation	Command	Description
Enter system view	**system-view**	-
Enable the SFTP client	**sftp** { *host-ip* | *host-name* } [*port-num*] [**prefer_kex** { **dh_group1** | **dh_exchange_group** } | **prefer_ctos_cipher** { **des** | **aes128** } | **prefer_stoc_cipher** { **des** | **aes128** } | **prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** } | **prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }]*	Required

Disabling the SFTP client

Table 622 Disable the SFTP client

Operation	Command	Description
Enter system view	**system-view**	-
Enter SFTP client view	**sftp** { *host-ip* | *host-name* }	-
Disable the SFTP client	**bye**	The three commands have the same function.
	exit	
	quit	

Operating with SFTP directories

SFTP directory-related operations include: changing or displaying the current directory, creating or deleting a directory, displaying files or information of a specific directory.

Table 623 Operate with SFTP directories

Operation	Command	Description
Enter system view	**system-view**	Optional
Enter SFTP client view	**sftp** { *host-ip* | *host-name* }	
Change the current directory	**cd** [*remote-path*]	
Return to the upper directory	**cdup**	
Display the current directory	**pwd**	
Display the list of the files in a directory	**dir** [**-a** | **-l**] [*remote-path*]	Optional
	ls [**-a** | **-l**] [*remote-path*]	The **dir** and **ls** commands have the same function.
Create a directory on the SFTP server	**mkdir** *remote-path*	Optional
Delete a directory from the SFTP server	**rmdir** *remote-path*&<1-10>	

Operating with SFTP files

SFTP file-related operations include: changing file name, downloading files, uploading files, displaying the list of the files, deleting files.

Table 624 Operate with SFTP files

Operation	Command	Description
Enter system view	**system-view**	Optional
Enter SFTP client view	**sftp** { *host-ip* | *host-name* }	
Rename a file or directory on the SFTP server	**rename** *old-name new-name*	
Download a file from the remote SFTP server	**get** *remote-file* [*local-file*]	
Upload a file to the remote SFTP server	**put** *local-file* [*remote-file*]	
Display the list of the files in a directory	**dir** [**-a** | **-l**] [*remote-path*]	Optional
	ls [**-a** | **-l**] [*remote-path*]	The **dir** and **ls** commands have the same function.
Delete a file from the SFTP server	**delete** *remote-file*&<1-10>	Optional
	remove *remote-file*&<1-10>	The **delete** and **remove** commands have the same function.

Displaying help information

You can display help information about a command, such as syntax and parameters.

Table 625 Display help information about SFTP client commands

Operation	Command	Description
Enter system view	**system-view**	-

Table 625 Display help information about SFTP client commands

Operation	Command	Description
Enter SFTP client view	**sftp** { *host-ip* | *host-name* }	-
Display help information about SFTP client commands	**help** [**all** | *command-name*]	Optional

SFTP Configuration Example

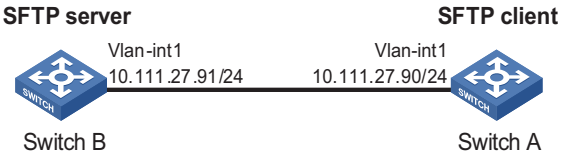
Network requirements

As shown in Figure 204.

- An SSH connection is present between Switch A and Switch B.
- Switch B serves as an SFTP server, with IP address 10.111.27.91/24.
- Switch A serves as an SFTP client, with IP address 10.111.27.90/24.
- An SSH username abc with password hello is created.

Network diagram

Figure 204 Network diagram for SFTP configuration



Configuration procedure

1 Configure Switch B (SFTP server)

Enable the SFTP server.

```
[SW7750] sftp server enable
```

Specify SFTP service for SSH user abc.

```
[SW7750] ssh user abc service-type sftp
```

2 Configure Switch A (SFTP client)

Establish a connection to the remote SFTP server and enter SFTP client view.

```
[SW7750] sftp 10.111.27.91
```

Display the current directory on the SFTP server, delete file z and verify the operation.

```
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey1
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
-rwxrwxrwx   1 noone    nogroup         0 Sep 01 08:00 z
Received status: End of file
Received status: Success
sftp-client> delete z
```

```
The following files will be deleted:
/z
Are you sure to delete it?(Y/N):y
This operation may take a long time.Please wait...

Received status: Success
File successfully Removed
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey1
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
Received status: End of file
Received status: Success
```

Create directory new1 and verify the operation.

```
sftp-client> mkdir new1
Received status: Success
New directory created
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey1
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
drwxrwxrwx   1 noone    nogroup         0 Sep 02 06:30 new1
Received status: End of file
Received status: Success
```

Rename directory new1 to new2 and verify the operation.

```
sftp-client> rename new1 new2
Received status:Success
File successfully renamed
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey1
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
drwxrwxrwx   1 noone    nogroup         0 Sep 02 06:33 new2
Received status: End of file
Received status: Success
```

Download file pubkey2 and rename it to public.

```
sftp-client> get pubkey2 public .....
This operation may take a long time, please wait...

Remote  file:/pubkey2 --->  Local file: public
Received status: End of file
Received status: Success...
Downloading file successfully ended
```

Upload file pu to the SFTP server and rename it to puk. Verify the operations.

```
sftp-client> put pu puk
This operation may take a long time, please wait...
Local file: pu --->  Remote file: /puk
Received status: Success
Uploading file successfully ended
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey1
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
drwxrwxrwx   1 noone    nogroup         0 Sep 02 06:33 new2
-rwxrwxrwx   1 noone    nogroup       283 Sep 02 06:35 pub
-rwxrwxrwx   1 noone    nogroup       283 Sep 02 06:36 puk
Received status: End of file
Received status: Success
sftp-client>
```

Exit from SFTP.

```
sftp-client> quit
Bye
[SW7750]
```

72 FILE SYSTEM MANAGEMENT

You can provide the directory argument in the following two ways in this chapter.

- *In the form of [drive] [path]. In this case, the argument can be a string containing 1 to 64 characters.*
- *By specifying the name of a storage device, such as flash:/ and cf:/.*

You can provide the *file-url* argument in the following two ways in this chapter.

- *In the form of [drive] [path] [file name]. In this case, the argument can be a string containing 1 to 64 characters.*
- *By specifying the name of a storage device, such as flash:/ and cf:/.*

File System Configuration

Introduction to File System

To facilitate management on storage devices such as the Flash of a switch, An Ethernet switch has the file system module built in. The file system allows you to access and manage files and directories, such as the operations of creating/deleting/modifying/renaming a file or a directory and displaying the contents of a file.

By default, a switch prompts for confirmation before executing the commands which have potential risks (for example, deleting and overwriting files).

Switch 7750s support Fabric switchover. Both the primary and the secondary Fabric have file system built in for you to manipulate the files on the both Fabrics. Note that the URL of a file on the secondary Fabric must begin with slot[No.]#flash:/, where No. is the number of the slot where the secondary Fabric is seated. Assume that the secondary Fabric is seated in slot 1, then you need to use slot1#flash:/text.txt to identify the file named text.txt and residing in the root directory of the secondary Fabric.

CF Module Configuration

You can use CF (compact flash) module on a Switch 7750 to extend the memory space. A CF module can be seated in the compact flash slot of a Fabric.

- With a CF module seated in the compact flash slot, you can access the root directory of the CF module by executing the **cd cf:** command.
- The commands used to manipulate files, such as **dir**, **copy**, **delete**, and **move**, apply to the files on a CF module.
- You can disable a CF module by using the **umount cf:** command. To use a disabled CF module again, you need to remove it and install it again.

Table 626 CF Module Configuration

Operation	Command	Description
Enter the root directory of a CF card	**cd cf:**	Required
Disable a CF card	**umount cf:**	Required

Currently, only the 96Gbps Switch Fabric supports the CF module.

The operations listed in Table 627 are available in the directories on a CF module.

File System Configuration Tasks

Table 627 File system configuration tasks

Task	Remark	Related section
Directory-related operations	Optional	"Directory-Related Operations" on page 792
File-related operations	Optional	"File-Related Operations" on page 792
Storage device-related operations	Optional	"Storage Device-Related Operations" on page 793
Setting the file system prompt mode	Optional	"Prompt Mode Configuration" on page 794

Directory-Related Operations

The file system provides directory-related operations, such as:

- Creating/deleting a directory
- Displaying the information about the files or the directories in the current directory or a specified directory

Table 628 lists the directory-related operations.

Table 628 Directory-related operations

Operation	Command	Description
Create a directory	**mkdir** *directory*	Optional
Delete a directory	**rmdir** *directory*	Optional Only empty directories can be deleted.
Display the current directory	**Pwd**	Optional
Display the information about specific directories and files	**dir** [/**all**] [*file-url*]	Optional
Enter a specified directory or switch to a specified storage device	**cd** *directory*	Optional

*In the output information of the **dir /all** command, deleted files (that is, those in the recycle bin) are embraced in brackets.*

File-Related Operations

The file system also provides file-related operations as listed in Table 629.

Table 629 File-related operations

Operation	Command	Description
Delete a file	**delete** [**/unreserved**] *file-url*	Optional A deleted file can be restored if you delete it by executing the **delete** command with the **/unreserved** keyword not specified. You can use the **undelete** command to restore a deleted file of this kind.
Restore a deleted file	**undelete** *file-url*	Optional This operation can only restore the files deleted with the **/unreserved** keyword not specified.
Delete a file in the recycle bin	**reset recycle-bin** [*file-url*] [**/force**]	Optional
Rename a file	**rename** *fileurl-source fileurl-dest*	Optional
Copy a file	**copy** *fileurl-source fileurl-dest*	Optional
Move a file	**move** *fileurl-source fileurl-dest*	Optional
Display the content of a file	**more** *file-url*	Optional Currently, the file system only supports displaying the contents of a file in texts.
Display the information about a directory or a file	**dir** [**/all**] [*file-url*]	Optional
Enter system view	**system-view**	-
Execute a batch file	**execute** *filename* [**echo on**]	Optional

CAUTION:

- *For deleted files whose names are the same, only the latest deleted file can be restored.*
- *The files which are deleted using the **delete** command with the **/unreserved** keyword not specified are actually moved to the recycle bin and thus still take storage space. You can clear the recycle bin to make room for other files by using the **reset recycle-bin** command.*
- *In the output information of the **dir /all** command, deleted files (that is, those in the recycle bin) are embraced in brackets.*
- *If the configuration files are deleted, the switch adopts the default configuration parameters when it starts the next time.*
- *The **execute** command cannot be executed recursively.*

Storage Device-Related Operations

With the file system, you can format a storage device, such as the Flash or a CF module. Note that the format operation leads to the loss of all files on the storage device and is irretrievable. For memory spaces that are unavailable due to unexpected errors, you can use the **fixdisk** command to restore them.

Table 630 Storage device-related operations

Operation	Command	Description
Format a storage device	**format** *device*	Required
Restore a storage device	**fixdisk** *device*	Optional

Prompt Mode Configuration

You can set the file system prompt mode to be **alert** or **quiet**. When in the **alert** mode, the file system prompts for confirmation when you perform irreversible operations (such as deleting a file completely or overwriting a file). If you are in the **quiet** mode, you are not prompted when you execute the operations.

Table 631 lists the operations to configure the file system prompt mode.

Table 631 Configuration on prompt mode of file system

Operation	Command	Description
Enter system view	**system-view**	-
Set the file system prompt mode	**file prompt** { **alert** | **quiet** }	Required By default, the file system prompt mode is **alert**.

File System Configuration Example

Display all the files in the root directory of the file system on the local unit.

```
<SW7750> dir /all
Directory of flash:/

   0   -rw-          4   Mar 09 2006 13:59:19   snmpboots
   1   -rw-  16215134    Apr 04 2006 16:36:20   S7750.app
   2   -rw-        483   Apr 20 2006 14:50:54   diaginfo.txt
   3   -rw-       3980   Apr 21 2006 15:08:29   config.cfg
   4   drw-          -   Apr 16 2006 11:18:17   hj
   5   drw-          -   Apr 10 2005 19:07:59   dd
   6   -rw-      11779  Apr 05 2006 10:23:03   test.bak
   7   -rw-      19307  Apr 16 2006 11:15:55   1.txt
   8   -rw-         66   Apr 05 2006 11:32:28   temp1

31877 KB total (15876 KB free)
```

Create a directory named test.

```
<SW7750> mkdir test
.
%Created dir flash:/test.
```

Copy flash:/config.cfg as flash:/test/1.cfg.

```
<SW7750> copy flash:/config.cfg flash:/test/1.cfg
......
%Copy file flash:/config.cfg to flash:/test/1.cfg...Done.
```

Display the file information.

```
<SW7750> dir /all
Directory of flash:/
```

```
   0   -rw-          4   Mar 09 2006 13:59:19   snmpboots
   1   -rw-  16215134    Apr 04 2006 16:36:20   S7750.app
   2   -rw-        483   Apr 20 2006 14:50:54   diaginfo.txt
   3   -rw-       3980   Apr 21 2006 15:08:29   config.cfg
   4   drw-          -   Apr 16 2006 11:18:17   hj
   5   drw-          -   Apr 10 2005 19:07:59   dd
   6   -rw-      11779  Apr 05 2006 10:23:03   test.bak
   7   -rw-      19307  Apr 16 2006 11:15:55   1.txt
   8   -rw-         66   Apr 05 2006 11:32:28   temp1
   9   drw-          -   Apr 25 2006 16:27:46   test

31877 KB total (15876 KB free)
<SW7750> dir flash:/test/
Directory of flash:/test/

   0   -rw-      3980  Apr 25 2006 16:33:21   1.cfg

31877 KB total (15869 KB free)
```

Enter directory test.

```
<SW7750> cd test
```

Rename 1.cfg as c.cfg.

```
<SW7750> rename 1.cfg c.cfg
.
%Renamed file flash:/1.cfg to flash:/c.cfg.
```

Delete the file c.cfg

```
<SW7750> delete c.cfg.

%Deleted file flash:/test/c.cfg.
```

Restore the file c.cfg.

```
<SW7750> undelete c.cfg
....
%Undeleted file flash:/test/c.cfg.
```

Display the content of the file c.cfg.

```
<SW7750>more c.cfg

#
 sysname 3Com Switch 7754
#
 local-server nas-ip 127.0.0.1 key 3Com
#
 domain default enable system
#
 temperature-limit 0 10 70
 temperature-limit 2 10 80
 temperature-limit 3 10 70
```

.....(Omitted)

73 BIMS CONFIGURATION

Introduction to BIMS

To manage a network device through SNMP or Telnet, you need to know its IP address. This is difficult however when the device obtains address through DHCP or when the device resides behind a NAT device. Branch intelligent management system (BIMS) was thus developed, delivering automatic configuration file and application update.

Basic Principles and Functions of BIMS

BIMS comprises the BIMS center side and the device side. The following is how it works to centralize device management:

1. The device sends the BIMS center a request at startup or/and sends requests at regular or irregular intervals. This depends on how you set your policy.
2. The BIMS center interacts with different devices according to the policy issued by the administrator. During interaction, the administrator can manage the device, for example, upgrade software, modify configuration, or view configuration/state information.

   At BIMS center side is service software operating on a PC or server, such as the BIMS component of 3Com's Quidview (V3.10). At BIMS device side the BIMS function is integrated in the software system of the router. By accessing the BIMS center, the router updates its configuration file and application automatically.

   BIMS allows the device to access the BIMS center immediately after the corresponding command is executed, at startup, at regular intervals, or at a specified time.

Update Procedure of Configuration File or Application

The following is how the device uses BIMS to update its configuration file or application, assuming that the BIMS configuration on the device is complete and BIMS is enabled:

1. The device sends a request to the BIMS center, asking for checking whether its files need update.
2. The BIMS center examines the device file information in the request. If update is needed, the BIMS center sends back a response containing information for update. This response may contain information such as URL for updating the configuration file or software or contain the commands and parameters that the device must execute.
3. The device checks the response. It gets the URL for obtaining device software, encrypted configuration file, or the commands and parameters to be executed.
4. After the device gets the configuration file, it executes and saves the configuration file.
5. Using the obtained URL, the device requests the BIMS center for downloading the device file.

6 The device verifies the device software obtained from the BIMS center and updates it to the local. Then the device sends an acknowledgement to the BIMS center.

7 Upon receipt of the acknowledgement, the BIMS center logs the event and sends back a response.

BIMS Device Configuration Tasks

BIMS is a convenient management tool. It provides an intelligent function for upgrading the configuration file and applications. BIMS device configuration involves the following two parts:

- Basic configuration. For details, see "Basic Configuration of BIMS Device" on page 798.
- Configuration of BIMS access mode. For details, see "Configuring BIMS Access Mode" on page 799.



CAUTION:

- *When you use the BIMS device to upgrade the host software and configuration file, the name of the file downloaded and saved to the local device is the same as that on the BIMS device.*
- *If the device experiences power failure during the upgrade of host software or configuration file, it is possible that old host software or configuration file is deleted and the new file is not saved yet. In this case, the upgrade will fail, the configuration on the device will be lost, and eventually the BIMS cannot manage the device.*

Basic Configuration of BIMS Device

Table 632 BIMS device basic configuration

Operation	Command	Description
Enter system view	**system-view**	-
Enable BIMS on the device	**bims enable**	Required By default, BIMS is disabled on the device.
Configure the unique identifier of the device	**bims device-id** *string*	Required By default, no unique identifier of the device is configured.
Configure the IP address and port number of the BIMS center	**bims ip address** *ip-address* [**port** *portnumber*]	Required By default, no IP address and port number of the BIMS center are configured.
Configure the shared key between the BIMS device and BIMS center	**bims sharekey** { **simple** | **cipher** } *sharekey*	Required By default, no shared key is configured.
Configure the source IP address in the packet sent by the BIMS device	**bims source ip-address** *ip-address*	Optional By default, no source IP address in the packet sent by the BIMS device is configured.



CAUTION: *The same port number must be configured on the BIMS device and on the BIMS center.*

Configuring BIMS Access Mode

Enabling BIMS Device to Access BIMS Center upon Power-on

After you make the following configuration, the BIMS device can access the BIMS center after it is powered on and initialized.

Table 633 Enable BIMS device to access BIMS center upon power-on

Operation	Command	Description
Enter system view	**system-view**	-
Enable BIMS device to access BIMS center upon power-on	**bims boot request**	Optional By default, if the BIMS is enabled on the device, the device can access the BIMS center immediately upon power-on.



If you disable the above access function on the device, the device will not send a message to the BIMS center after the device is restarted. Therefore, the BIMS center cannot detect that the device is restarted and still display the message, indicating that it is waiting for restart of the device.

Configuring Interval for Accessing the BIMS Center

You can configure the BIMS device to access the BIMS center at regular intervals.

Table 634 Configure the BIMS device to access the BIMS center at regular intervals

Operation	Command	Description
Enter system view	**system-view**	-
Configure the interval for accessing the BIMS center	**bims interval** *number*	Optional By default, no BIMS center accessing interval is set.

When the BIMS device is configured with an access interval different than the one set at the BIMS center, it obtains and uses the setting on the BIMS center for later accesses. The likelihood exists that this interval is obtained by multiple BIMS devices. This, however, does not result in excessive concurrent accesses, because the BIMS center has a tuning mechanism to handle the situation.

Accessing the BIMS Center at a Specified Time

You can configure the BIMS device to access the BIMS center at a specified time and if desired, at regular intervals from then on during a specified period.

Table 635 Configure the device to access the BIMS center at a specified time

Operation	Command	Description
Enter system view	**system-view**	-
Configure the BIMS device to access the BIMS center at the specified time If desired, configure the device to access the BIMS center from then on at regular intervals during a specified period	**bims specify-time** *start-time* [[*end-time*] **period** *numberdays*]	Optional By default, no specific time that the BIMS device accesses the BIMS center is configured.

Accessing the BIMS Center as Driven by the Command

Execute the following command in system view to enable the BIMS device access the BIMS center immediately.

Table 636 Enable the device to access the BIMS center immediately

Operation	Command	Description
Enter system view	**system-view**	-
Enable the device to access the BIMS center immediately	**bims request**	Optional

BIMS Configuration Example

Configuring the BIMS Device to Access the BIMS Center Periodically at Startup

Network requirements

The BIMS device accesses the BIMS center at startup and from then on every 48 hours.

The BIMS center is implemented using the BIMS component of 3Com Quidview NMS. Its IP address and port number are 10.153.21.97 and 80 respectively.

Configuration procedure

1 Configure the BIMS center

- Set the shared key used between the BIMS center and the BIMS device. This shared key must be the same as the one configured on the BIMS device.
- Add the BIMS device to the NMS manually or automatically.
  - Manual mode: You enter the device name manually to add this device to the system.
  - Auto mode: Enable the "Automatically add the device" function and set the shared key between the BIMS center and BIMS device. After that, when the device accesses the BIMS center, it can be automatically added to the BIMS center.
- Specify the files for upgrade, including configuration file and application. When the device accesses the BIMS center, the BIMS center will judge whether to use these files to upgrade the files on the device. If yes, the BIMS center sends these files to the device to upgrade the files on the device



For detailed configuration procedures, refer to the part discussing the BIMS component in Quidview Network Management System User Manual.

2 Configure the BIMS device

Enter system view.

```
<SW7750> system-view
```

Enable BIMS.

```
[SW7750] bims enable
  bims is enable
```

Assign the device a unique identifier ar18-20-907.

```
[SW7750] bims device-id ar18-20-907
```

Configure the shared key used between the BIMS center and device.

```
[SW7750] bims sharekey simple 1122334455667788
```

Configure the IP address of the BIMS. The default port 80 is used.

```
[SW7750] bims ip address 10.153.21.97
```

Configure the interval for accessing the BIMS center.

```
[SW7750] bims interval 2880
```

Configuring the BIMS Device to Access the BIMS Center Periodically within a Specified Period

Network requirements

The BIMS device will access the BIMS center at 12:10 on May 1, 2005. From then on, it will access the BIMS center every two days until 23:50 on October 1, 2005.

The IP address and port number of the BIMS center are 10.153.21.97 and 80 respectively.

Configuration procedure

1 Configure the BIMS center

Refer to "Configuring the BIMS Device to Access the BIMS Center Periodically at Startup" on page 800.

2 Configure the BIMS device

Enter system view.

```
<SW7750> system-view
```

Enable BIMS.

```
[SW7750] bims enable
  bims is enable
```

Assign the device a unique identifier ar18-20-907.

```
[SW7750] bims device-id ar18-20-907
```

Configure the shared key used between the BIMS center and device.

```
[SW7750] bims sharekey simple 1122334455667788
```

Configure the IP address of the BIMS. The default port 80 is used.

```
[SW7750] bims ip address 10.153.21.97
```

Configure the device to access the BIMS center at 12:10 on May 1, 2005, and from then on at two-day interval until October 1, 2005 23:50.

```
[SW7750] bims specify-time 12:10 2005/05/01 23:50 2005/10/01 period 2
```

74 FTP AND TFTP CONFIGURATION

FTP Configuration

Introduction to FTP

FTP (file transfer protocol) is commonly used in IP-based networks to transmit files. Before World Wide Web comes into being, files are transferred through command lines, and the most popular application is FTP. At present, although E-mail and Web are the usual methods for file transmission, FTP still has its strongholds.

As an application layer protocol, FTP is used for file transfer between remote server and local host. TCP port 21 is used for control connections, and port 20 is used for data connections. Basic FTP operations are described in RFC 959.

FTP-based file transmission is performed in the following two modes:

- Binary mode, which is used for program file transfer.
- ASCII mode, which is used for text file transfer.

An Ethernet switch can act as an FTP client or an FTP server in an FTP implementation.

- FTP server

An Ethernet switch can operate as an FTP server to provide file transmission services for FTP clients. You can log into a switch operating as an FTP server by running an FTP client program on your PC to access the files on the FTP server. To accept login requests, an FTP server must be assigned an IP address.

Table 637 describes the configurations needed when a switch operates as an FTP server.

Table 637 Configurations needed when a switch operates as an FTP server

Device	Configuration	Default	Description
Switch	Enable the FTP server function	The FTP server function is disabled by default	You can run the **display ftp-server** command to view the FTP server configuration on the switch.
	Perform authentication-/authorization-related configuration	By default, FTP server logon authentication and authorization are not configured.	Configure user names, passwords, and the work directory.
	Configure the connection idle time	The default idle time is 30 minutes.	-

Table 637 Configurations needed when a switch operates as an FTP server

Device	Configuration	Default	Description
PC	Log into a switch operating as an FTP server through an FTP client application.	-	-

CAUTION: *The FTP-related functions require that the route between a FTP client and the FTP server is reachable.*

- FTP client

A switch can operate as an FTP client, through which you can access files on FTP servers. In this case, you need to establish a connection between your PC and the switch through a terminal emulation program or Telnet and then execute the **ftp** X.X.X.X command on your PC (*X.X.X.X* is the IP address of an FTP server).

Table 638 describes the configurations needed when a switch operates as an FTP client.

Table 638 Configurations needed when a switch operates as an FTP client

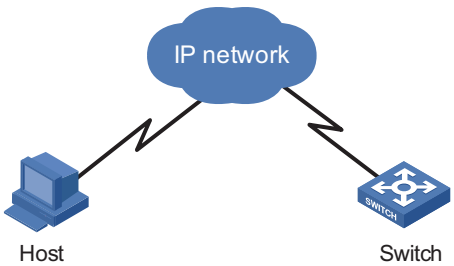
Device	Configuration	Default	Description
Switch	Run the **ftp** command to log into a remote FTP server directly	-	To log into a remote FTP server and manipulate files and directories on it, you need to obtain a user name and password first.
FTP server	User names, passwords, and the corresponding permissions are configured.	-	-

FTP Configuration: A Switch Operating as an FTP Server

Prerequisites

A switch operates as an FTP server. A remote PC operates as an FTP client. The network operates properly, as shown in Figure 205.

Figure 205 Network diagram for FTP configuration



Configuration procedure

Table 639 Configure an FTP server

Operation	Command	Description
Enter system view	**system-view**	-
Enable the FTP server function	**ftp server enable**	Required By default, the FTP server function is disabled.
Set the connection idle time	**ftp timeout** *minutes*	Optional The default connection idle time is 30 minutes.

- *Only one user can access a Switch 7750 at a given time when the latter operates as an FTP server.*
- *FTP services are implemented in this way: An FTP client sends FTP requests to the FTP server. The FTP server receives the requests, perform operations accordingly, and return the results to the FTP client.*
- *To prevent unauthorized accesses, an FTP server disconnects a FTP connection when it does not receive requests from the FTP client for a specific period of time known as the connection idle time.*
- *A Switch 7750 operating as an FTP server cannot receive a file whose size exceeds its storage space. A client attempting to upload such a file will be disconnected from the FTP server due to lack of storage space on the FTP server.*

Authentication and authorization configuration

An FTP server authenticates an FTP client by the user name and the password it provides. When an FTP client passes the authentication, the authorization is done by allocating the FTP client a work directory. An FTP server provides services to the FTP clients that are both authenticated and authorized.

The configurations such as configuring user name, password, the way to display passwords, service type are performed on FTP servers. Refer to the information about the **local-user**, **local-user password-display-mode**, **password**, and **service-type** commands in "Configuring the Attributes of a Local User" on page 523.

Displaying FTP server configuration

After the above configurations, you can run the **display** command in any view to display the information about the FTP server and verify your configurations.

Table 640 Display FTP server information

Operation	Command	Description
Display the information about FTP server configurations on a switch	**display ftp-server**	These commands can be executed in any view.
Display the currently online FTP client	**display ftp-user**	

Configuration Example: A Switch Operating as an FTP Server

Network requirements

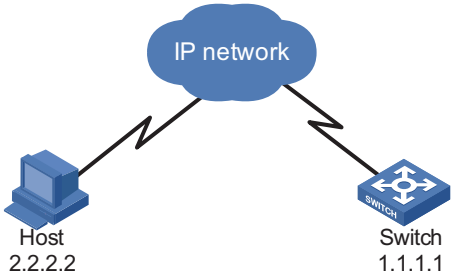
A switch operates as an FTP server and a remote PC as an FTP client.

- Create a user account on the FTP server with the user name "switch" and password "hello". The work directory assigned for FTP clients is the root directory of the flash.
- Configure the IP address 1.1.1.1 for a VLAN interface on the switch, and 2.2.2.2 for the PC. Ensure the route between the two is reachable.

The switch application named switch.app is stored on the PC. Upload it to the FTP server through FTP to upgrade the application of the switch, and download the switch configuration file named config.cfg from the switch to backup the configuration file.

Network diagram

Figure 206 Network diagram for FTP configurations



Configuration procedure

1 Configure the switch

Log into the switch. (You can log into a switch through the Console port or by Telneting to the switch. See "Logging into an Ethernet Switch" on page 33 for detailed information.)

```
<SW7750>
```

Start the FTP service on the switch and create a user account and the corresponding password.

```
<SW7750> system-view
[SW7750] ftp server enable
[SW7750] local-user switch
[SW7750-luser-switch] password simple hello
[SW7750-luser-switch] service-type ftp ftp-directory flash:/
```

2 Run an FTP client application on the PC to connect to the FTP server. Upload the application named switch.app to the root directory of the Flash memory of the FTP server, and download the configuration file named config.cfg from the FTP server. The following takes the command line window tool provided by Windows as an example.

Enter the command line window and switch to the directory where the file switch.app is located. Assume that the file resides in C:.

```
C:\>
```

Access the Ethernet switch through FTP. Input the user name "switch" and password "hello" to log in and enter FTP view.

```
C:\> ftp 1.1.1.1
Connected to 1.1.1.1.
220 FTP service ready.
User (1.1.1.1:(none)): switch
331 Password required for switch.
Password:
230 User logged in.
ftp>
```

Upload the switch.app file.

```
ftp> put switch.app
200 Port command okay.
150 Opening ASCII mode data connection for switch.app.
226 Transfer complete.
```

Download the config.cfg file.

```
ftp> get config.cfg
200 Port command okay.
150 Opening ASCII mode data connection for config.cfg.
226 Transfer complete.
ftp: 3980 bytes received in 8.277 seconds 0.48Kbytes/sec.
```

This example uses the command line window tool provided by Windows. When you log into the FTP server through another FTP client, refer to the corresponding instructions for operation description.



CAUTION:

- *If the available space of the flash of the switch is not enough to hold the file to be uploaded, you need to move the files that are not in use from the flash to other place to make room for the file.*
- *3Com series switch is not shipped with FTP client applications. You need to purchase and install it by yourself.*

3 After uploading the application, you can update the application on the switch.

Use the **boot boot-loader** command to specify the uploaded file (switch.app) to be the startup file used when the switch starts the next time, and restart the switch. Thus the switch application is upgraded.

```
<SW7750> boot boot-loader switch.app
<SW7750> reboot
```



*For information about the **boot boot-loader** command and how to specify the startup file for a switch, refer to "Specifying the APP to be Adopted at Reboot" on page 863.*

FTP Configuration: A Switch Operating as an FTP Client

The function for a switch to operate as an FTP client is implemented by an application module built in the switch. Thus a switch can operate as an FTP client without any configuration. You can perform FTP-related operations (such as creating/removing a directory) by executing FTP client commands on a switch

operating as an FTP client. Table 641 lists the operations that can be performed on an FTP client.

Table 641 Basic FTP client configuration

Operation	Command	Description
Enter FTP client view	**ftp** [**cluster** | *ftp-server* [*port-number*]]	-
Specify to transfer files in the ASCII mode	**ascii**	Optional By default, files are transferred in ASCII characters.
Specify to transfer files in the binary mode	**binary**	Optional
Specify to transfer files in the passive mode	**passive**	Optional By default, the passive mode is adopted.
Change the work directory on the remote FTP server	**cd** *pathname*	Optional
Change the work directory to the parent directory	**cdup**	Optional
Get the local work directory on the FTP client	**lcd**	Optional
Display the directories on the FTP server	**pwd**	Optional
Create a directory on the remote FTP server	**mkdir** *pathname*	Optional
Remove a directory on the remote FTP server	**rmdir** *pathname*	Optional
Delete a specified file	**delete** *remotefile*	Optional
Query a specified file	**dir** [*filename*] [*localfile*]	Optional
Query a specified remote file	**ls** [*remotefile*] [*localfile*]	Optional The **ls** command does not support extended parameters, such as -a.
Download a remote file	**get** *remotefile* [*localfile*]	Optional
Upload a local file to the remote FTP server	**put** *localfile* [*remotefile*]	Optional
Switch to another FTP user	**user** *username* [*password*]	Optional
Establish a control connection to the FTP server	**open** { *ip-address* | *server-name* } [*port*]	Optional
Terminate the current FTP connection without exiting FTP client view	**disconnect**	Optional
Terminate the current FTP connection without exiting FTP client view	**close**	Optional
Terminate the current FTP connection and quit to user view	**quit**	Optional
Terminate the current FTP connection and quit to user view	**bye**	Optional

Table 641 Basic FTP client configuration

Operation	Command	Description
Display the on-line help on a specified command concerning FTP	**remotehelp** [*protocol-command*]	Optional
Enable debugging for FTP	**debugging**	Optional
Enable the verbose function	**verbose**	Optional The verbose function is enabled by default.

Configuration Example: A Switch Operating as an FTP Client

Network requirements

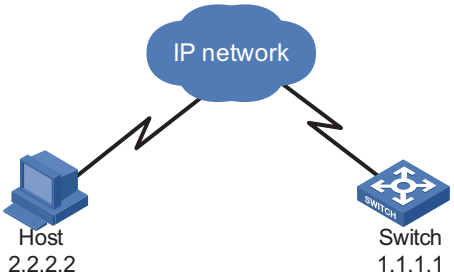
A switch operates as an FTP client and a remote PC as an FTP server.

- Create a user account on the FTP server with the user name "switch" and password "hello", and authorize the user "switch" with read and write permissions on the directory named "switch" on the PC.
- Configure the IP address 1.1.1.1 for a VLAN interface on the switch, and 2.2.2.2 for the PC. Ensure the route between the two is reachable.

The switch application named switch.app is stored on the PC. Download it to the switch through FTP to upgrade the switch application, and upload the switch configuration file named config.cfg to the PC to backup the configuration file.

Network diagram

Figure 207 Network diagram for FTP configuration



Configuration procedure

1 Perform FTP server-related configurations on the PC, that is, create a user account on the FTP server with user name "switch" and password "hello". (For detailed configuration, refer to the configuration instruction relevant to the FTP server software.)

2 Configure the switch.

Log into the switch. (You can log into a switch through the Console port or by Telneting to the switch. See "Logging into an Ethernet Switch" on page 33 for detailed information.)

```
<SW7750>
```

CAUTION: *If the available space of the flash of the switch is not enough to hold the file to be uploaded, you need to move the files that are not in use from the flash to other place to make room for the file.*

Connect to the FTP server using the **ftp** command. You need to provide the IP address of the FTP server, the user name and the password as well.

```
<SW7750> ftp 2.2.2.2
Trying ...
Press CTRL+K to abort
Connected.
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User(none):switch
331 Give me your password, please
Password:
230 Logged in successfully
[ftp]
```

Run the **put** command to upload the configuration file named config.cfg to the FTP server.

```
[ftp] put config.cfg
```

Run the **get** command to download the file named switch.app to the flash of the switch.

```
[ftp] get switch.app
```

Run the **quit** command to terminate the FTP connection and quit to user view.

```
[ftp] quit
<SW7750>
```

Run the **boot boot-loader** command to specify the downloaded file (switch.app) to be the startup file used when the switch starts the next time, and then restart the switch. Thus the switch application is upgraded.

```
<SW7750> boot boot-loader switch.app
<SW7750> reboot
```



*For information about the **boot boot-loader** command and how to specify the startup file for a switch, refer to "Specifying the APP to be Adopted at Reboot" on page 863.*

TFTP Configuration

Introduction to TFTP

Compared with FTP, TFTP (trivial file transfer protocol) features simple interactive access interface and no authentication control. It simplifies the interaction between servers and clients remarkably. TFTP is implemented on UDP. It transfers data through UDP port 69. Basic TFTP operations are described in RFC1986.

TFTP transmission is initiated by clients, as described in the following:

- To download a file, a client sends read request packets to the TFTP server, receives data from the TFTP server, and then sends acknowledgement packets to the TFTP server.
- To upload a file, a client sends writing request packets to the TFTP server, sends data to the TFTP server, and then receives acknowledgement packets from the TFTP server.

- *Before performing TFTP-related configurations, you need to configure IP addresses for the TFPT client and the TFTP server, and make sure the route between the two is reachable.*
- *A switch can only operate as a TFTP client.*

Figure 208 Network diagram for TFTP configuration

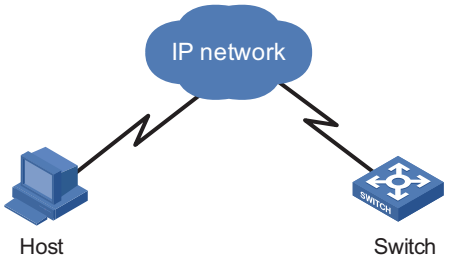


Table 642 describes the operations needed when a switch operates as a TFTP client.

Table 642 Configurations needed when a switch operates as a TFTP client

Device	Configuration	Default	Description
Switch	Configure an IP address for the VLAN interface of the switch so that it is reachable for TFTP server.	-	TFTP applies to networks where client-server interactions are comparatively simple. It requires the routes between TFTP clients TFTP servers are reachable.
	You can log into a TFTP server directly for file accessing through TFTP commands.	-	-
TFTP server	The TFTP server is started and the TFTP work directory is configured.	-	-

TFTP Configuration

Prerequisites

A switch operates as a TFTP client and a remote PC as the TFTP server. The network operates properly, as shown in Figure 208.

Basic TFTP configurations

Table 643 Basic TFTP configurations

Operation	Command	Description
Download a file through TFTP	**tftp** { **cluster** | *tftp-server* } **get** *source-file* [*dest-file*]	Optional
Upload a file through TFTP	**tftp** { **cluster** | *tftp-server* } **put** *source-file* [*dest-file*]	Optional
Enter system view	**system-view**	-

Table 643 Basic TFTP configurations

Operation	Command	Description
Specify the ACL adopted when a switch attempts to connect a TFTP server	**tftp-server acl** *acl-number*	Optional

TFTP Configuration Example

Network requirements

A switch operates as a TFTP client and a PC as the TFTP server.

- The TFTP work directory is configured on the TFTP server.
- The IP address of a VLAN interface on the switch is 1.1.1.1. The port through which the switch connects with the PC belongs to the VLAN. The IP address of the PC is 1.1.1.2.

The application named switch.app is stored on the PC. Download it to the switch through TFTP, and upload the configuration file named config.cfg to the work directory on the PC to backup the configuration file.

Network diagram

Figure 209 Network diagram for TFTP configuration



Configuration procedure

1 Start the TFTP server and configure the work directory on the PC.

2 Configure the switch.

Log into the switch. (You can log into a switch through the Console port or by Telneting to the switch. See "Logging into an Ethernet Switch" on page 33 for detailed information.)

```
<SW7750>
```

CAUTION: *If the available space of the flash of the switch is not enough to hold the file to be uploaded, you need to move the files that are not in use from the flash to other place to make room for the file.*

Download the switch application named switch.app from the TFTP server to the switch.

```
<SW7750> tftp 1.1.1.2 get switch.app switch.app
```

Upload the switch configuration file named config.cfg to the TFTP server.

```
<SW7750> tftp 1.1.1.2 put config.cfg config.cfg
```

Use the **boot boot-loader** command to specify the downloaded file (switch.app) to be the startup file used when the switch starts the next time, and restart the switch. Thus the switch application is upgraded.

```
<SW7750> boot boot-loader switch.app
<SW7750> reboot
```



*For information about the **boot boot-loader** command and how to specify the startup file for a switch, refer to "Specifying the APP to be Adopted at Reboot" on page 863.*

75 INFORMATION CENTER

Information Center Overview

Information center is an indispensable part of Ethernet switches and exists as an information hub of system software modules. The information center manages most information outputs; it sorts information carefully, and hence can screen information in an efficient way. Combined with the debugging program (**debugging** commands), it provides powerful support for network administrators and developers in network operation monitoring and fault diagnosis.

Information items output by Switch 7750s are presented in the following format:

```
<priority>timestamp sysname module/level/digest:content
```

Here, angle brackets "<>", spaces, slashes "/" and colon are the fixed format of information.

Below is an example of log output to a log host:

```
<188>Apr  9 17:28:50:524 2004 3Com IFNET/5/UPDOWN:Line protocol on t
he interface M-Ethernet0/0/0 is UP    (SIP=10.5.1.5 ,SP=1080)
```

The following describes the fields of an information item:

1 Priority

The calculation formula for priority is priority = facility × 8 + severity - 1. in which

- facility (the device name) defaults to local7 with the value being 23 (the value of local6 is 22, that of local5 is 21, and so on).
- severity (the information level) ranges from 1 to 8. Table 645 details the value and meaning associated with each severity.

Note that no character is permitted between the priority and time stamp. The priority takes effect only when the information is sent to the log host.

2 Time stamp

The time stamp sent to the log host is in the format of Mmm dd hh:mm:ss yyyy, where:

Mmm" represents the month, and the available values are: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov and Dec.

dd" is the date, which shall follow a space if less than 10, for example, "7".

hh:mm:ss" is the local time, where "hh" is in the 24-hour format, ranging from 00 to 23, both "mm" and "ss" range from 00 to 59.

yyyy" is the year.

Note that a space separates the time stamp and host name.

3 Host name

It refers to the system name of the host, which is "3Com" by default.

You can modify the host name with the **sysname** command. Refer to "Setting the System Name of the Switch" on page 853.

Note that a space separates the host name and module name.

4 Module name

It indicates the modules that generate the information. The module name is in abbreviation form to indicate different modules. Table 644 lists the name and description of some modules generating information.

Table 644 Modules generating information

Module name	Description
ACCOUNT	L3+ real-time accounting module
ACL	Access control list module
ADBM	Address base module
AM_USERB	Access management module
ARP	Address resolution protocol module
BGP	Border gateway protocol module
CFM	Configuration file management module
CLNP	Connectionless network protocol module
CLNSECHO	Connectionless network protocol echo module
CLST	Cluster management module
CMD	Command line module
DEV	Device management module
DHCP	Dynamic host configuration protocol module
DHCPS	DHCP server module
DHCPSNP	DHCP snooping module
DIAG	Diagnostics module
DLDP	Device link detection protocol module
DNS	Domain name system module
ENTEXMIB	Entity extended MIB module
ENTITY	Entity module
ESIS	End system to intermediate system routing protocol module
ETH	Ethernet module
FIB	Forwarding module
FTPS	FTP server module

Table 644 Modules generating information

Module name	Description
HA	High availability module
HABP	3Com authentication bypass protocol module
HWCM	3Com Configuration Management private MIB module
HWP	NQA module
IFNET	Interface management module
IGSP	IGMP snooping module
IP	Internet protocol module
IPX	IPX protocol module
ISIS	Intermediate system-to-intermediate system intra-domain routing information exchange protocol module
L2INF	Layer 2 interface management module
LACL	Lanswitch access control list module
LARP	Address Resolution protocol module
LETH	Ethernet debugging module
LINKAGG	Link aggregation module
LQOS	Lanswitch quality of service module
LS	Local server module
MIX	Dual main control network management protocol
MODEM	MODEM module
MPM	Multicast port management module
MSDP	Multicast source discovery protocol module
MSTP	Multiple spanning tree protocol module
NAT	Network address translation module
NDP	Neighbor discovery protocol module
NETSTREA	Traffic statistic module
NTDP	Network topology discovery protocol module
NTP	Network time protocol module
OSPF	Open shortest path first module
RDS	Radius module
RM	Routing management module
RMON	Remote monitor module
RMX	IPX routing module
RRPP	Rapid ring protection protocol module
RSA	Revest, Shamir and Adleman encryption module
RTA	L3+ plug-in module traffic accounting module
RTPRO	Routing protocol module
RXTX	Lower layer packets receiving and transmitting module
SC	Server control module
SHELL	User interface module
SNMP	Simple network management protocol module
SOCKET	Socket module
SSH	Secure shell module

Table 644 Modules generating information

Module name	Description
SYSM	System management module
SYSMIB	System MIB module
TAC	Terminal access controller module
TELNET	Telnet module
TFTPC	TFTP client module
TUNNEL	Packets transparent transmission module
UDPH	UDP helper module
USERLOG	User log module
VFS	Virtual file system module
VLAN	Virtual local area network module
VRRP	VRRP (virtual router redundancy protocol) module
VTY	VTY (virtual type terminal) module
default	Default settings for all the modules

Note that a slash (/) separates the module name and severity level.

5 Severity

Switch information falls into three categories: log information, debugging information and trap information. The information center classifies the information into eight levels by severity or emergency. The higher the information severity is, the lower the corresponding level is. For example, the "debugging" severity corresponds to level 8, and the "emergencies" severity corresponds to level 1. If filtered by severity, the information of a severity level greater than the defined threshold will be filtered out for output. Therefore, when the severity threshold is set to "debugging", all information will be output. See Table 645 for description of severities and corresponding levels.

Table 645 Severity definitions on the information center

Severity	Value	Description
emergencies	1	The system is unavailable.
alerts	2	Errors that need to be corrected immediately
critical	3	Critical errors
errors	4	Common errors
warnings	5	Warnings
notifications	6	Normal information that needs to be noticed
informational	7	Normal prompt information
debugging	8	Debugging information

Note that a slash (/) separates the level and digest.

6 Digest

It is a phrase within 32 characters, abstracting the information contents.

A colon (:) separates the digest and information contents.

7 Information text

Information text contains the detail of system information.

The above section describes the log information format sent to a log server by a switch. Some log server software will resolve the received information as well as its format, so that you may see the log format displayed on the log server is different from the one described in this manual.

Information Center Configuration

The switch supports information output to six directions, and the system defaults to assign one information channel for each output direction, as shown in Table 646.

Table 646 Information channel names and numbers

Output direction	Channel number	Default channel name
Console	0	console
Monitor terminal	1	monitor
Log host	2	loghost
Trap buffer	3	trapbuffer
Log buffer	4	logbuffer
SNMP	5	snmpagent

Settings for the six output directions are independent. However, for any output direction, you must first enable the information center function to make all other settings effective.

Information center of the Ethernet switch features:

- Supporting six information output directions, namely, console (console), monitor terminal (monitor), log host (loghost), trap buffer (trapbuffer), log buffer (logbuffer) and SNMP (snmp agent).
- Filtering information by information severities (information is divided into eight severity levels).
- Filtering information by modules where information is generated.
- Language options (Chinese or English) for information output to a log host.

Enabling Information Output to a Log Host

Table 647 lists the related configurations on the switch.

Table 647 Enable information output to a log host

Operation	Command	Description
Enter system view	**system-view**	-
Enable the information center	**info-center enable**	Optional By default, the information center is enabled.

Table 647 Enable information output to a log host

Operation	Command	Description
Enable information output to a log host	**info-center loghost** *host-ip-addr* [**channel** { *channel-number* | *channel-name* } | **facility** *local-number* | **language** { **chinese** | **english** }] *	Required By default, the switch does not output information to the log host. After you configure the switch to output information to the log host, the switch uses information channel 2 by default. Be sure to set the correct IP address. A loopback IP address will cause an error message prompting invalid address.
Configure the source interface through which log information is sent to the log host	**info-center loghost source** *interface-type interface-number*	Optional
Define an information source	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** } * { **level** *severity* | **state** *state* } *]	Required
Set the format of the time stamp	**info-center timestamp** { **log** | **trap** | **debugging** } { **boot** | **date** | **none** }	Optional

*To view the debugging information of specific modules, you need to set the information type as **debug** in the **info-center source** command, and enable debugging for corresponding modules through the **debugging** command.*

Enabling Information Output to the Console

Table 648 lists the related configurations on the switch.

Table 648 Enable information output to the console

Operation	Command	Description
Enter system view	**system-view**	-
Enable the information center	**info-center enable**	Optional By default, the information center is enabled.
Enable information output to the console	**info-center console channel** { *channel-number* | *channel-name* }	Required By default, the switch uses information channel 0 to output log/debugging/trap information to the console.
Define an information source	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** } { **level** *severity* | **state** *state* }]*	Required

Table 648 Enable information output to the console

Operation	Command	Description
Set the format of time stamp	**info-center timestamp** { **log** | **trap** | **debugging** } { **boot** | **date** | **none** }	Optional

To view debugging/log/trap output information on the console, you should also enable the corresponding debugging/log/trap information terminal display on the switch.

For example, to view log information of the switch on the console, you should not only enable log information output to the console, but also enable log information terminal display with the **terminal logging** command.

Perform the following operations in user view.

Table 649 Enable debugging/log/trap terminal display

Operation	Command	Description
Enable the debugging/log/trap information terminal display function	**terminal monitor**	Optional By default, this function is enabled for console user.
Enable debugging information terminal display function	**terminal debugging**	Optional By default, the debugging information terminal display is disabled for terminal users.
Enable log information terminal display function	**terminal logging**	Optional By default, log information terminal display is enabled for console users.
Enable trap information terminal display function	**terminal trapping**	Optional By default, trap information terminal display is enabled for terminal users.

Enabling Information Output to a Monitor Terminal

Table 650 lists the related configurations on the switch.

Table 650 Enable information output to a monitor terminal

Operation	Command	Description
Enter system view	**system-view**	-
Enable the information center	**info-center enable**	Optional By default, the information center is enabled.
Enable information output to Telnet terminal or dumb terminal	**info-center monitor channel** { *channel-number* | *channel-name* }	Required By default, a switch outputs log/debugging/trap information to user terminal through information channel 1.

Table 650 Enable information output to a monitor terminal

Operation	Command	Description
Define an information source	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** } { **level** *severity* | **state** *state* }]*	Required
Set the format of time stamp	**info-center timestamp** { **log** | **trap** | **debugging** } { **boot** | **date** | **none** }	Optional This is to set the time stamp format for log/debugging/trap information output. This determines how the time stamp is presented to users.



- *When there are multiple Telnet users or dumb terminal users, some configuration parameters (including module filter, language and severity level threshold settings) are shared between them. In this case, change to any such parameter made by one user will also be reflected on all other user terminals.*
- *To view debugging information of specific modules, you need to set the information type as **debug** when defining the information source, and enable debugging for corresponding modules through the **debugging** command as well.*

To view the debugging/log/trap output information on the monitor terminal, you should enable the corresponding debugging/log/trap display function on the switch.

For example, to view log information of the switch on a monitor terminal, you need to not only enable log information output to the monitor terminal, but also enable log information terminal display function with the **terminal logging** command.

Perform the following configuration in user view.

Table 651 Enable debugging/log/trap terminal display

Operation	Command	Description
Enable the debugging/log/trap information terminal display function	**terminal monitor**	Optional By default, this function is enabled for console user.
Enable debugging information terminal display function	**terminal debugging**	Optional By default, debugging information terminal display is disabled for terminal users.
Enable log information terminal display function	**terminal logging**	Optional By default, log information terminal display is enabled for console users.

Table 651 Enable debugging/log/trap terminal display

Operation	Command	Description
Enable trap information terminal display function	**terminal trapping**	Optional By default, trap information terminal display is enabled for terminal users.

Enabling Information Output to the Log Buffer

Table 652 lists the related configurations on the switch.

Table 652 Enable information output to the log buffer

Operation	Command	Description
Enter system view	**system-view**	-
Enable the information center	**info-center enable**	Optional By default, the information center is enabled.
Enable information output to the log buffer	**info-center logbuffer** [**channel** { *channel-number* | *channel-name* } | **size** *buffersize*]* [**| exclude** *regular-expression*]	Optional By default, the switch uses information channel 4 to output log information to the log buffer, which can holds up to 512 items by default.
Define an information source	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** } { **level** *severity* | **state** *state* }]*	Required
Set the format of time stamp	**info-center timestamp** { **log** | **trap** | **debugging** } { **boot** | **date** | **none** }	Optional This is to set the time stamp format for log/debugging/trap information output. This determines how the time stamp is presented to users.

*To view debugging information of specific modules, you need to set the information type as **debug** in the **info-center source** command, and enable debugging on corresponding modules with the **debugging** command as well.*

Enabling Information Output to the Trap Buffer

Table 653 lists the related configurations on the switch.

Table 653 Enable information output to the trap buffer

Operation	Command	Description
Enter system view	**system-view**	-
Enable the information center	**info-center enable**	Optional By default, the information center is enabled.

Table 653 Enable information output to the trap buffer

Operation	Command	Description
Enable information output to the trap buffer	**info-center trapbuffer** [**channel** { *channel-number* | *channel-name* } | **size** *buffersize*]*	Optional By default, the switch uses information channel 3 to output trap information to the trap buffer, which can holds up to 256 items by default.
Define an information source	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** } { **level** *severity* | **state** *state* }]*	Required
Set the format of time stamp	**info-center timestamp** { **log** | **trap** | **debugging** } { **boot** | **date** | **none** }	Optional This is to set the time stamp format for log/debugging/trap information output. This determines how the time stamp is presented to users.

*To view debugging information of specific modules, you need to set the information type as **debug** in the **info-center source** command, and enable debugging on corresponding modules with the **debugging** command as well.*

Enabling Information Output to the SNMP

Table 654 lists the related configurations on the switch.

Table 654 Enable information output to the SNMP

Operation	Command	Description
Enter system view	**system-view**	-
Enable the information center	**info-center enable**	Optional By default, the information center is enabled.
Enable information output to the SNMP	**info-center snmp channel** { *channel-number* | *channel-name* }	Required By default, the switch outputs trap information to SNMP through channel 5.
Define an information source	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** } { **level** *severity* | **state** *state* }]*	Required
Set the format of time stamp	**info-center timestamp** { **log** | **trap** | **debugging** } { **boot** | **date** | **none** }	Optional This is to set the time stamp format for log/debugging/trap information output. This determines how the time stamp is presented to users.

- *To view debug information of specific modules, you need to set the information type as **debug** in the **info-center source** command, and enable debugging on corresponding modules with the **debugging** command as well.*
- *To send information to remote SNMP workstation properly, related configurations are required on both the switch and the SNMP workstation.*

Displaying and Debugging Information Center Configuration

After the above configurations, you can execute the **display** command in any view to display the running status of the information center, and thus validate you configurations. You can also execute the **reset** command in user view to clear the information in the log buffer and trap buffer.

Table 655 Display and debug information center

Operation	Command	Description
Display information on information channel	**display channel** [*channel-number* | *channel-name*]	The **display** command can be executed in any view
Display the operation status of information center, the configuration of information channels, the format of time stamp	**display info-center**	
Display the status of log buffer and the information recorded in log buffer	**display logbuffer** [**level** *severity* | **size** *buffersize*]* [**|** { **begin** | **exclude** | **include** } *regular-expression*]	
Display the summary information recorded in log buffer	**display logbuffer summary** [**level** *severity*]	
Display the status of trap buffer and the information recorded in trap buffer	**display trapbuffer** [**size** *buffersize*]	
Clear information recorded in log buffer	**reset logbuffer**	The **reset** command can be executed in user view
Clear information recorded in trap buffer	**reset trapbuffer**	

Information Center Configuration Examples

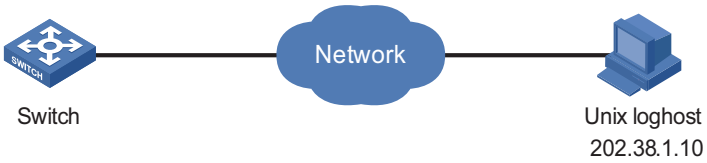
Log Output to a Unix Log Host

Network requirements

The switch sends the following log information in English to the Unix log host whose IP address is 202.38.1.10: the log information of the two modules ARP and IP, with severity higher than "informational".

Network diagram

Figure 210 Network diagram for log output to a Unix log host



Configuration procedure

1 Configure the switch:

Enable the information center.

```
<SW7750> system-view
[SW7750] info-center enable
```

Disable for all modules the function of outputting information to log host channels.

```
[SW7750] undo info-center source default channel loghost
```

Configure the host whose IP address is 202.38.1.10 as the log host. Set the output language to English. Permit ARP and IP modules to output information with severity level higher than informational to the log host.

```
[SW7750] info-center loghost 202.38.1.10 facility local4 language english
[SW7750] info-center source arp channel loghost log level informational debug sta
te off trap state off
[SW7750] info-center source ip channel loghost log level informational debug stat
e off trap state off
```

2 Configure the log host:

The operations here are performed on SunOS 4.0. The operations on other manufacturers' Unix operation systems are similar.

Step 1: Execute the following commands as the superuser (root user).

```
# mkdir /var/log/3Com
# touch /var/log/3Com/information
```

Step 2: Edit the file "/etc/syslog.conf" as the superuser (root user) to add the following selector/action pair.

```
# 3Com configuration messages
local4.info     /var/log/3Com/information
```

When you edit the file "/etc/syslog.conf", note that

- *A note must start in a new line following a "#" sign.*
- *In each pair, a tab should be used as a separator instead of a space.*
- *No space is allowed at the end of a file name.*
- *The facility and received log information severity level specified in the file "/etc/syslog.conf" must be the same as those corresponding parameters*

*configured in the commands **info-center loghost** and **info-center source**. Otherwise, log information may not be output to the log host normally.*

Step 3: After the log file "information" is created and the file "/etc/syslog.conf" is modified, run the following command to send a HUP signal to the system daemon "syslogd", so that it reads its new configuration file "/etc/syslog.conf".

```
# ps -ae | grep syslogd
147
# kill -HUP 147
```

After all the above operations, the switch can make records in the corresponding log file.

Through combined configuration of the device name (facility), information severity level threshold (severity), module name (filter) and file "syslog.conf", you can sort information precisely for filtering.

Log Output to a Linux Log Host

Network requirements

The switch sends the following log information in English to the Linux log host whose IP address is 202.38.1.10: All modules' log information, with severity higher than "errors".

Network diagram

Figure 211 Network diagram for log output to a Linux log host



Configuration procedure

1 Configure the switch:

Enable the information center.

```
<SW7750> system-view
[SW7750] info-center enable
```

Configure the host whose IP address is 202.38.1.10 as the log host. Set the output language to English. Permit all modules to output information with severity level higher than error to the log host.

```
[SW7750] info-center loghost 202.38.1.10 facility local7 language english
[SW7750] info-center source default channel loghost log level errors debug state
off trap state off
```

2 Configure the log host:

Step 1: Execute the following commands as the superuser (root user).

```
# mkdir /var/log/3Com
# touch /var/log/3Com/information
```

Step 2: Edit the file "/etc/syslog.conf" as the superuser (root user) to add the following selector/action pair.

```
# 3Com configuration messages
local7.info     /var/log/3Com/information
```

Note the following items when you edit file "/etc/syslog.conf".

- A note must start in a new line following a "#" sign.
- In each pair, a tab should be used as a separator instead of a space.
- No space is permitted at the end of the file name.
- The facility and received log information severity specified in file "/etc/syslog.conf" must be the same with those corresponding parameters configured in commands **info-center loghost** and **info-center source**. Otherwise, log information may not be output to the log host normally.

Step 3: After the log file "information" is created and the file "/etc/syslog.conf" is modified, run the following commands to view the process ID of the system daemon "syslogd", stop the process, and then restart the daemon "syslogd" in the background with the "-r" option.

```
# ps -ae | grep syslogd
147
# kill -9 147
# syslogd -r &
```

In case of Linux log host, the daemon "syslogd" must be started with the "-r" option.

After all the above operations, the switch can make records in the corresponding log file.

Through combined configuration of the device name (facility), information severity level threshold (severity), module name (filter) and file "syslog.conf", you can sort information precisely for filtering.

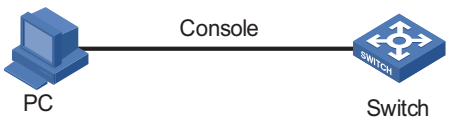
Log Output to the Console

Network requirements

The switch sends the following information to the console: the log information of the two modules ARP and IP, with severity higher than "informational".

Network diagram

Figure 212 Network diagram for log output to the console



Configuration procedure

Enable the information center.

```
<SW7750> system-view
[SW7750] info-center enable
```

Disable for all modules the function of outputting information to the console channels.

```
[SW7750] undo info-center source default channel console
```

Enable log information output to the console. Permit ARP and IP modules to output information with severity level higher than informational to the console.

```
[SW7750] info-center console channel console
[SW7750] info-center source arp channel console log level informational
[SW7750] info-center source ip channel console log level informational
```

Enable terminal display.

```
<SW7750> terminal monitor
<SW7750> terminal logging
```

76 DNS CONFIGURATION

DNS Overview

Domain name system (DNS) is a distributed database system that provides domain name-to-IP address mappings for TCP/IP applications. With DNS, users using IP applications can directly use meaningful easy-to-remember domain names, which will be resolved and mapped to corresponding IP addresses by DNS servers.

There are two types of DNS resolution, "Static DNS Resolution" on page 831 and "Dynamic DNS Resolution" on page 831. When a name query is received, the static resolution is first performed to check the static DNS list. If the static resolution fails, the dynamic resolution is performed. Because dynamic resolution needs the participating of DNS server and may spend some time, you can put some commonly used domain names in the static DNS list to increase the resolution efficiency.

Static DNS Resolution

With static DNS resolution, you can manually configure some name-to-address mappings in the static DNS list, and the system will search the static list for corresponding IP addresses when users use domain names with some applications (such as telnet).

Dynamic DNS Resolution

Resolving procedure

The procedure of dynamic DNS resolution is as follows:

1. A user program sends a name query to the resolver in the DNS Client.
2. The DNS resolver looks up the local DNS cache for a match. If a match is found, it returns the corresponding IP address to the user program. If not, it sends a query to the DNS Server.
3. The DNS Server looks up its database for a match. If no match is found, it sends a query to its parent DNS Server. If the parent DNS Server does not have the information, it sends the query to another server. This process continues until a result (either successful or failed) is found. Finally, the resolution result is returned to the DNS Client.
4. The DNS Client performs the next operation according to the result.

Figure 213 Dynamic DNS resolution

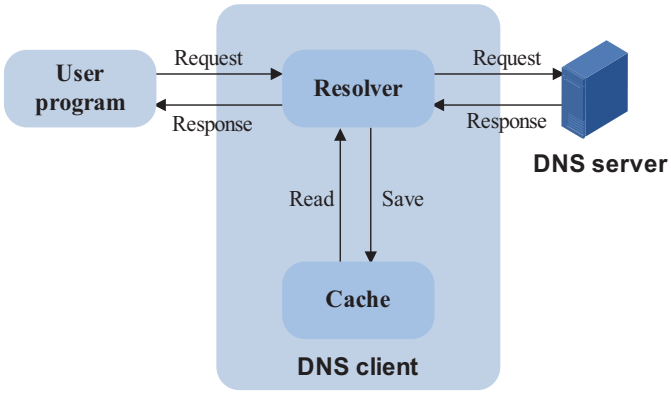


Figure 213 shows the relationship between the user program, DNS Client and DNS Server.

The resolver and cache compose the DNS Client. The user program runs on the same machine as the DNS client, while the DNS Server and the DNS Client must run on different machines.

Dynamic DNS resolution allows the DNS Client to store the latest name-to-address mappings in the dynamic domain name cache. So there is no need to send a request to the DNS Server for the same domain next time. The DNS Client removes aged mappings from the cache, so as to obtain updated mappings from the DNS Server. The setting on the DNS Server determines the aging time, and the DNS Client gets the information from DNS messages.

DNS suffix list

The DNS Client normally holds a DNS suffix list where you can define some domain name suffixes. It is used when the name to be resolved is not complete. The resolver can use the list to supply the missing part. For example, you can configure a suffix "com" in the list, and users only need to input "aabbcc" to get the IP address of aabbcc.com, for the resolver will automatically add the suffix and delimiter before passing the name to the DNS Server.

When a user input a domain name:

- If there is no dot in the domain name, such as "aabbcc", the resolver will consider this as a host name and add a suffix to the name before performing DNS lookup. If all the suffixes in the DNS suffix list have been tried but no DNS lookup succeeds, the resolver will use the original name (such as aabbcc) for a DNS lookup.
- If there is a dot in the domain name, such as "www.aabbcc" or "aabbcc.", the resolver will first use this domain name to perform DNS lookup before trying any other suffix.

Currently, the Switch 7750 Ethernet switches support both static and dynamic domain name resolution on the DNS Client.

If you have configured aliases for domain names on the DNS server, the Ethernet switch can resolve a host IP address according to its alias.

Configuring Static DNS Resolution

Table 656 Configure static DNS resolution

Operation	Command	Description
Enter system view	system-view	-
Add a hostname-to-address mapping entry	**ip host** *hostname ip-address*	Required There is no entry in the static DNS list by default.

As one hostname can mapped to only one IP address, when you add multiple hostname-to-address mapping entries with the same hostname, only the last one will be valid.

You can add up to 50 entries for static DNS resolution.

Configuring Dynamic DNS Resolution

Configuration Procedure

Table 657 Configure dynamic DNS resolution

Operation	Command	Description
Enter system view	**system-view**	-
Enable dynamic DNS resolution	**dns resolve**	Required This function is disabled by default.
Configure a DNS server IP address	**dns server** *ip-address*	Required No DNS server IP address is configured by default.
Configure a DNS suffix	**dns domain** *domain-name*	Optional No DNS suffix is configured by default.

You can configure up to 6 DNS servers and 10 DNS suffixes.

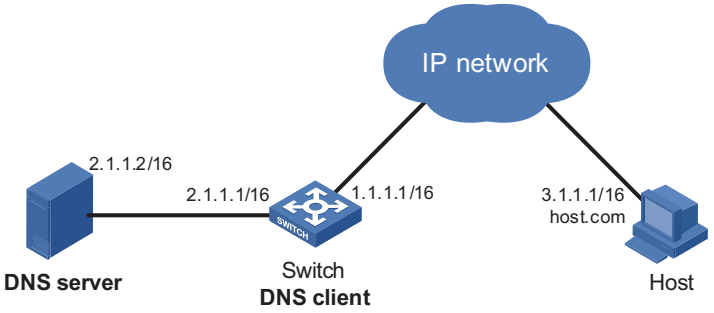
DNS Configuration Example

Network requirements

As shown in Figure 214, Switch is used as a DNS client with dynamic DNS resolution. It allows you to visit Host with IP address 3.1.1.1/16. The DNS server IP address is 2.1.1.2/16. The DNS suffixes “com” and “net” are configured.

Network diagram

Figure 214 Network diagram for dynamic DNS resolution



Configuration procedure

Before doing the following configuration, suppose the route between Switch and Host is reachable, the DNS server works normally, and a mapping entry from Host to IP address 3.1.1.1/16 exists on the DNS server.

Enable dynamic DNS resolution.

```
<SW7750> system-view
[SW7750] dns resolve
```

Configure the DNS server IP address 2.1.1.2.

```
[SW7750] dns server 2.1.1.2
```

Configure net as a DNS suffix.

```
[SW7750] dns domain net
```

Configure com as a DNS suffix.

```
[SW7750] dns domain com
```

Ping Host on Switch to verify the configuration and the corresponding IP address (it should be 3.1.1.1).

Displaying and Maintaining DNS

After the above configuration, you can execute the **display** command in any view to view the DNS configuration and running information to verify your configuration.

You can execute the **reset** command in user view to clear the dynamic DNS cache.

Table 658 Display and maintain DNS

Operation	Command	Description
Display static DNS list information	**display ip host**	You can execute the **display** command in any view.
Display DNS server information	**display dns server** [**dynamic**]	
Display DNS suffix list information	**display dns domain**	
Display dynamic DNS cache information	**display dns dynamic-host**	
Clear the dynamic DNS cache.	**reset dns dynamic-host**	Execute the **reset** command in user view.

Troubleshooting DNS Configuration

Symptom

Dynamic DNS resolution is enabled, but the user cannot get the correct IP address from a domain name.

Analysis

DNS client needs to be used in conjunction with the DNS server to get the correct IP address through domain name resolution.

Solution

- Use the **display dns dynamic-host** command to check if the specified domain name is in the cache.
- If the specified domain name is in the cache, but the IP address is wrong, ensure that the DNS Client has the correct IP address of the DNS Server.
- If the specified domain name is not in the cache, ensure that dynamic DNS resolution is enabled, the DNS Client can normally communicate with the DNS Server, and the DNS Server works normally.
- Check the DNS mapping list is correct on the DNS Server.

77 BOOTROM AND HOST SOFTWARE LOADING

Traditionally, the loading of switch software is accomplished through a serial port. This approach is slow, inconvenient, and cannot be used for remote loading. To resolve these problems, the TFTP and FTP modules are introduced into the switch. With these modules, you can load/download software/files conveniently to the switch through an Ethernet port.

This chapter introduces how to load BootROM and host software to a switch locally and how to do this remotely.

Introduction to Loading Approaches

You can load software locally by using:

- XMODEM through Console port
- TFTP through Ethernet port
- FTP through Ethernet port

You can load software remotely by using:

- FTP
- TFTP

The BootROM software version should be compatible with the host software version when you load the BootROM and host software.

Local Software Loading

If your terminal is directly connected to the switch, you can load the BootROM and host software locally.

Before loading the software, make sure that your terminal is correctly connected to the switch to insure successful loading.

The loading process of the BootROM software is the same as that of the host software, except that during the former process, you should press <Ctrl+U> and <Enter> after entering the Boot Menu and the system gives different prompts. The following text mainly describes the BootROM loading process.

Boot Menu

```
Starting......
RAMLine.....OK
System is booting...................


            ****************************************
            *                                      *
            *    3Com Switch 7757 BOOTROM, Version 530      *
```

```
            *                                        *
            ******************************************

Copyright(c) 2004-2007 3Com Corporation
Creation date   : Apr 15 2007, 14:48:52
CPU type        : MPC8245
CPU Clock Speed : 300Mhz
BUS Clock Speed : 33Mhz
BOOT_FLASH type : AMD29LV040B
Flash  Size     : 32MB
Memory Size     : 256MB



S7757 main board self testing.............................
SDRAM Data lines Selftest.................................OK!
SDRAM Address lines Selftest..............................OK!
SDRAM fast selftest.......................................OK!
Please check LEDs.....................LEDs selftest finished!
CPLD selftest.............................................OK!
FPGA selftest.............................................OK!
The switch Mac address is ......................000F.E22E.5576



Press Ctrl+B to enter Boot Menu... 5
```

Press <Ctrl+B>. The system displays:

```
Password :
```

To enter the Boot Menu, you should press <Ctrl+B> within five seconds after the information "Press Ctrl-B to enter Boot Menu..." appears. Otherwise, the system starts to decompress the program; and if you want to enter the Boot Menu at this time, you will have to restart the switch.

Input the correct BootROM password (no password is need by default). The system enters the Boot Menu:

```
BOOT  MENU

1. Download application file to flash
2. Select application file to boot
3. Display all files in flash
4. Delete file from flash
5. Modify bootrom password
0. Reboot

Enter your choice(0-5):
```

Loading Software Using XMODEM through Console Port

Introduction to XMODEM

XMODEM is a file transfer protocol that is widely used due to its simplicity and good performance. XMODEM transfers files via Console port. It supports two types of data packets (128 bytes and 1 KB), two check methods (checksum and CRC), and multiple attempts of error packet retransmission (generally the maximum number of retransmission attempts is ten).

The XMODEM transmission procedure is completed by a receiving program and a sending program: The receiving program sends negotiation characters to negotiate a packet checking method. After the negotiation, the sending program starts to transmit data packets. When receiving a complete packet, the receiving program checks the packet using the agreed method. If the check succeeds, the receiving program sends an acknowledgement character and the sending program proceeds to send another packet; otherwise, the receiving program sends a negative acknowledgement character and the sending program retransmits the packet.

Loading BootROM software

Follow these steps to load the BootROM software:

Step 1: At the prompt "Enter your choice(0-5):" in the Boot Menu, press <Ctrl+U>, and then press <Enter> to enter the BootROM update menu shown below:

```
SRPG bootrom update menu:

1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return to boot menu

Enter your choice(0-3):
```

Then you can choose different protocols to load BootROM.

Step 2: Enter 3 in the above menu to download the BootROM software using XMODEM. The system will prompt to enter the name of the BootROM file to load.

```
Load File name           :S7750.btm
```

The system displays the following download baud rate setting menu:

```
Please select your download baudrate:
1: 9600
2: 19200
3: 38400
4: 57600
5: 115200
0: Return

Enter your choice(0-5):
```

Step 3: Choose an appropriate download baud rate. For example, if you enter 5, the baud rate 115200 bps is chosen and the system displays the following information:

```
Download baudrate is 115200 bps
Please change the terminal's baudrate to 115200 bps and select XMODEM protocol
Press enter key when ready
```



If you have chosen 9600 bps as the download baud rate, you need not modify the HyperTerminal's baud rate, and therefore you can skip Step 4 and 5 below and

proceed to Step 6 directly. In this case, the system will not display the above information.

Following are configurations on PC. Take the Hyperterminal using Windows operating system as example.

Step 4: Choose [File/Properties] in HyperTerminal, click <Configure> in the pop-up dialog box, and then select the baud rate of 115200 bps in the Console port configuration dialog box that appears, as shown in Figure 215, Figure 216.

Figure 215 Properties dialog box

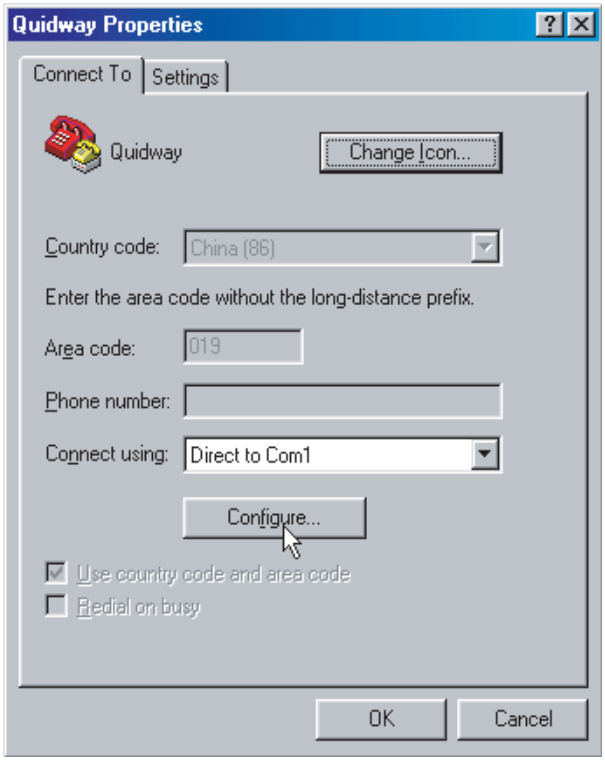
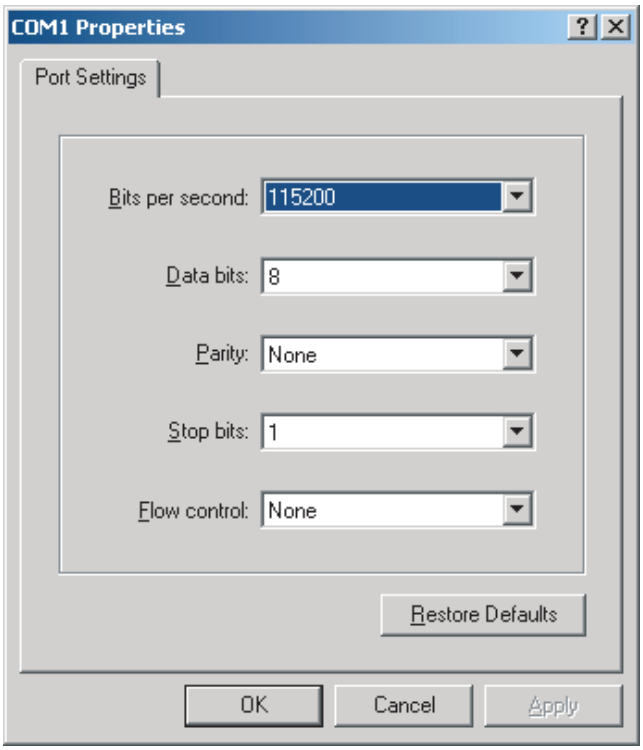
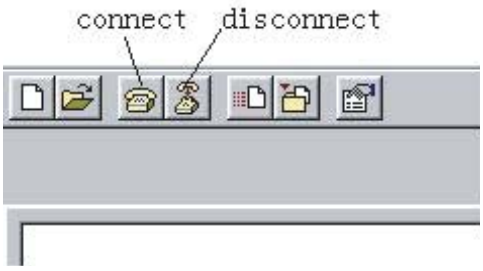


Figure 216 Console port configuration dialog box



Step 5: Click the <Disconnect> button to disconnect the HyperTerminal from the switch and then click the <Connect> button to reconnect the HyperTerminal to the switch, as shown in Figure 217.

Figure 217 Connect and disconnect buttons



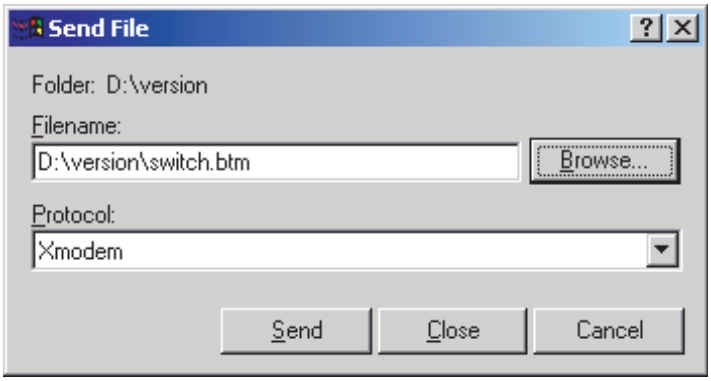
The new baud rate takes effect only after you disconnect and reconnect the HyperTerminal program.

Step 6: Press <Enter> to start downloading the program. The system displays the following information:

```
Now please start transfer file with XMODEM protocol.
If you want to exit, Press <Ctrl+X>.
Loading ...CCCCCCCCCC
```

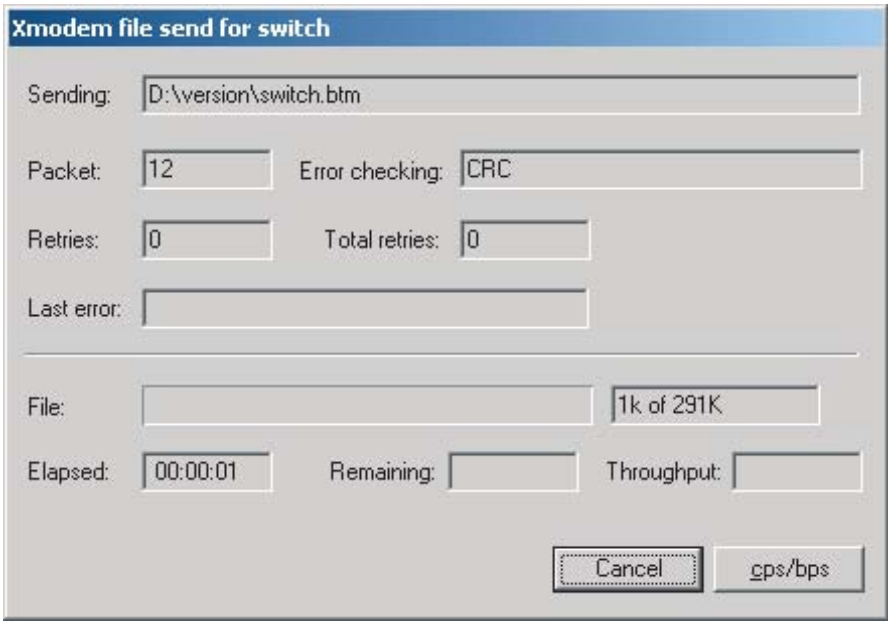
Step 7: Choose [Transfer/Send File] in the HyperTerminal's window, and click <Browse> in pop-up dialog box, as shown in Figure 218. Select the software you need to download, and set the protocol to XMODEM.

Figure 218 Send file dialog box



Step 8: Click <Send>. The system displays the page, as shown in Figure 219.

Figure 219 Sending file page



Step 9: After the download completes, the system displays the following information:

```
Loading ...CCCCCCCCCC done!
```

Step 10: Reset HyperTerminal's baud rate to 9600 bps (refer to Step 4 and 5). Then, press any key as prompted. The system will display the following information when it completes the loading.

```
Bootrom updating.....................................done!
```

- *If the HyperTerminal's baud rate is not reset to 9600 bps, the system prompts "Your baudrate should be set to 9600 bps again! Press enter key when ready".*
- *You need not reset the HyperTerminal's baud rate and can skip the last step if you have chosen 9600 bps. In this case, the system upgrades BootROM automatically and prompts "Bootrom updating now.....done!".*

Loading host software

Follow these steps to load the host software:

Step 1: Select <1> in Boot Menu and press <Enter>. The system displays the following information:

```
1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return to boot menu

Enter your choice(0-3):
```

Step 2: Enter 3 in the above menu to download the host software using XMODEM.

The subsequent steps are the same as those for loading the BootROM software, except that the system gives the prompt for host software loading instead of BootROM loading.

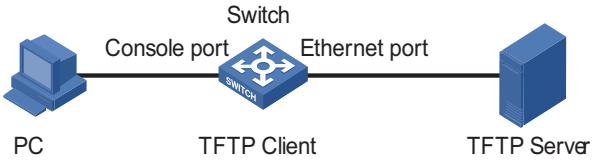
Loading Software Using TFTP through Ethernet Port

Introduction to TFTP

TFTP, one protocol in TCP/IP protocol suite, is used for trivial file transfer between client and server. It uses UDP to provide unreliable data stream transfer service.

Loading BootROM software

Figure 220 Local loading using TFTP



Step 1: As shown in Figure 220, connect the switch through an Ethernet port to the TFTP server, and connect the switch through the Console port to the configuration PC.

You can use one PC as both the configuration device and the TFTP server.

Step2: Run the TFTP server program on the TFTP server, and specify the path of the program to be downloaded.

CAUTION: *TFTP server program is not provided with the 3Com Series Ethernet Switches.*

Step 3: Run the HyperTerminal program on the configuration PC. Start the switch. Then enter the Boot Menu.

At the prompt "Enter your choice(0-5):" in the Boot Menu, press <Ctrl+U>, and then press <Enter> to enter the BootROM update menu shown below:

```
SRPG bootrom update menu:

1. Set TFTP protocol parameter
```

```
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return to boot menu

Enter your choice(0-3):
```

Step 4: Enter 1 to in the above menu to download the BootROM software using TFTP. Then set the following TFTP-related parameters as required:

```
Load File name           :S7750.btm
Switch IP address        :1.1.1.2
Server IP address        :1.1.1.1
```

Step 5: Press <Enter>. The system displays the following information:

```
Are you sure you want update SRPG bootrom?Yes or No(Y/N)
```

Step 6: Enter Y to start file downloading or N to return to the Bootrom update menu. If you enter Y, the system begins to download and update the BootROM software. Upon completion, the system displays the following information:

```
Prepare for loading...OK!
Loading.....................................done
Bootrom updating.........done!
```

Loading host software

Follow these steps to load the host software.

Step 1: Select <1> in Boot Menu and press <Enter>. The system displays the following information:

```
1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return to boot menu

Enter your choice(0-3):3
```

Step 2: Enter 1 in the above menu to download the host software using TFTP.

The subsequent steps are the same as those for loading the BootROM program, except that the system gives the prompt for host software loading instead of BootROM loading.



CAUTION: *When loading BootROM and host software using Boot menu, you are recommended to use the PC directly connected to the device as TFTP server to promote upgrading reliability.*

Loading Software Using FTP through Ethernet Port

Introduction to FTP

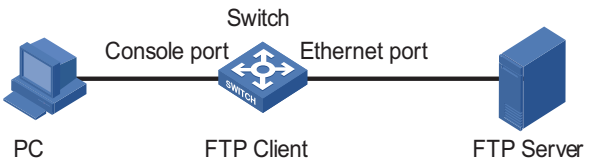
FTP is an application-layer protocol in the TCP/IP protocol suite. It is used for file transfer between server and client, and is widely used in IP networks.

You can use the switch as an FTP client or a server, and download software to the switch through an Ethernet port. The following is an example.

Loading Process Using FTP Client

- Loading BootROM software

Figure 221 Local loading using FTP client



Step 1: As shown in Figure 221, connect the switch through an Ethernet port to the FTP server, and connect the switch through the Console port to the configuration PC.

You can use one computer as both configuration device and FTP server.

Step 2: Run the FTP server program on the FTP server, configure an FTP user name and password, and copy the program file to the specified FTP directory.

Step 3: Run the HyperTerminal program on the configuration PC. Start the switch. Then enter the Boot Menu.

At the prompt "Enter your choice(0-5):" in the Boot Menu, press <Ctrl+U>, and then press <Enter> to enter the BootROM update menu shown below:

```
SRPG bootrom update menu:

1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return to boot menu

Enter your choice(0-3):
```

Step 4: Enter 2 in the above menu to download the BootROM software using FTP. Then set the following FTP-related parameters as required:

```
Load File name             :S7750.btm
Switch IP address          :10.1.1.2
Server IP address          : 10.1.1.1
FTP User Name              :7500
FTP User Password          :abc
```

Step 5: Press <Enter>. The system displays the following information:

```
Are you sure you want update SRPG bootrom?Yes or No(Y/N)
```

Step 6: Enter Y to start file downloading or N to return to the Bootrom update menu. If you enter Y, the system begins to download and update the program. Upon completion, the system displays the following information:

```
Prepare for loading...OK!
Loading.....................................done
Bootrom updating.........done!
```

- Loading host software

Follow these steps to load the host software:

Step 1: Select <1> in Boot Menu and press <Enter>. The system displays the following information:

```
1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return to boot menu
Enter your choice(0-3):
```

Enter 2 in the above menu to download the host software using FTP.

The subsequent steps are the same as those for loading the BootROM program, except for that the system gives the prompt for host software loading instead of BootROM loading.

CAUTION: *When loading BootROM and host software using Boot menu, you are recommended to use the PC directly connected to the device as TFTP server to promote upgrading reliability.*

Remote Software Loading

If your terminal is not directly connected to the switch, you can telnet to the switch, and use FTP or TFTP to load BootROM and host software remotely.

Remote Loading Using FTP

Loading Process Using FTP Client

1 Loading BootROM

As shown in Figure 222, a PC is used as both the configuration device and the FTP server. You can telnet to the switch, and then execute the FTP commands to download the BootROM program s7500.btm from the remote FTP server (with an IP address 10.1.1.1) to the switch.

Figure 222 Remote loading using FTP



Step 1: Download the software to the switch using FTP commands.

```
<SW7750> ftp 10.1.1.1
Trying ...
Press CTRL+K to abort
Connected.
220 FTP service ready.
User(none):abc
331 Password required for abc.
Password:
230 User logged in.
[ftp] get s7500.btm
200 Port command okay.
150 Opening ASCII mode data connection for s7500.btm.
...226 Transfer complete.
```

```
FTP: 1177900 byte(s) received in 4.594 second(s) 256.39K byte(s)/sec.
[ftp] bye
```

When using different FTP server software on PC, different information will be output to the switch.

Step 2: Update the BootROM program on Fabric of the switch.

```
<SW7750> boot bootrom s7500.btm slot 0
 This will update BootRom file on board 0 . Continue? [Y/N] y
 Board 0 upgrading BOOTROM, please wait...
 Upgrade board 0 BOOTROM succeeded!
```

Step 3: Restart the switch.

```
<SW7750> reboot
```

Before restarting the switch, make sure you have saved all other configurations that you want, so as to avoid losing configuration information.

2 Loading host software

Loading the host software is the same as loading the BootROM program, except for that the file to be downloaded is the host software file, and that you need to use the **boot boot-loader** command to select the host software at reboot of the switch.

After the above operations, the BootROM and host software loading is completed.

Pay attention to the following:

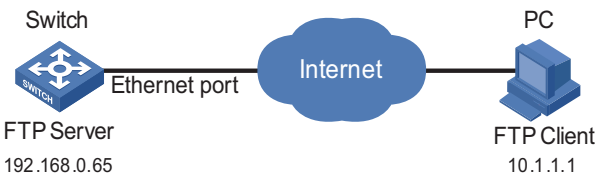
- The loading of BootROM and host software takes effect only after you restart the switch with the **reboot** command.
- If the space of the Flash memory is not enough, you can delete the useless files in the Flash memory before software downloading.
- No power-down is permitted during software loading.

Loading Process Using FTP Server

As shown in Figure 223, the switch is used as the FTP server. You can telnet to the switch, and then execute the FTP commands to download the BootROM program s7500.btm from the switch.

1 Loading BootROM

Figure 223 Remote loading using FTP server



Step 1: As shown in Figure 223, connect the switch through an Ethernet port to the PC (with IP address 10.1.1.1)

Step 2: Configure the IP address of VLAN1 on the switch to 192.168.0.65, and subnet mask to 255.255.255.0.

You can configure the IP address for any VLAN on the switch for FTP transmission. However, before configuring the IP address for a VLAN interface, you have to make sure whether the IP addresses of this VLAN and PC are routable.

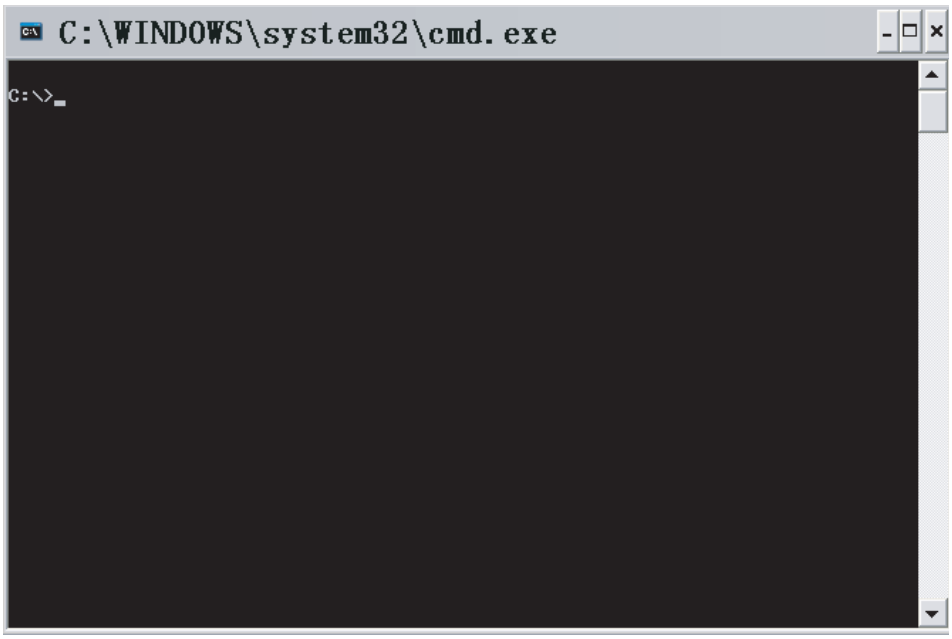
```
<SW7750> system-view
System View: return to User View with Ctrl+Z.
[SW7750] interface Vlan-interface 1
[SW7750-Vlan-interface1] ip address 192.168.0.65 255.255.255.0
```

Step 3: Enable FTP service on the switch, configure the FTP user name to test, password to pass, and directory to FLASH root directory.

```
[SW7750-Vlan-interface1] quit
[SW7750] ftp server enable
[SW7750] local-user test
New local user added.
[SW7750-luser-test] password simple pass
[SW7750-luser-test] service-type ftp ftp-directory flash:/
```

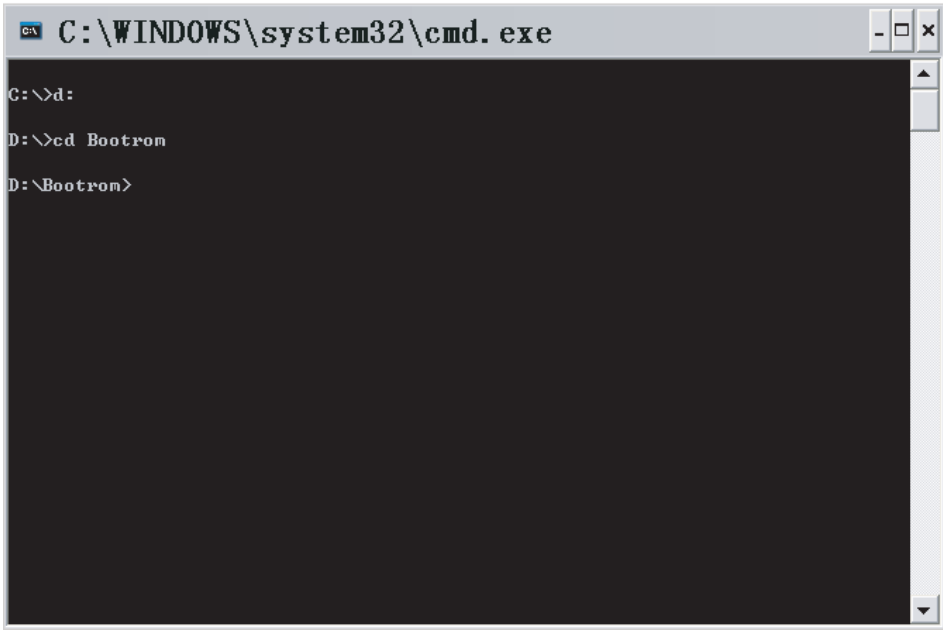
Step 4: Enable FTP client software on PC. Refer to Figure 224 for the command line interface in Windows operating system.

Figure 224 Command line interface



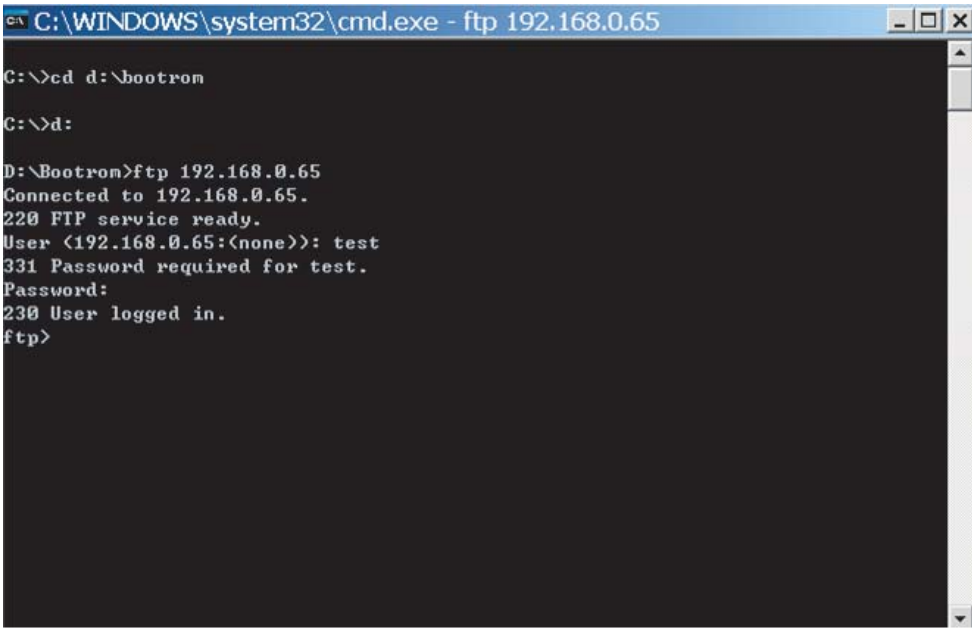
Step 5: Enter cd in the interface to switch to the path that the BootROM upgrade file is to be stored, and assume the name of the path is "D:Bootrom", as shown in Figure 225.

Figure 225 Switch to BootROM



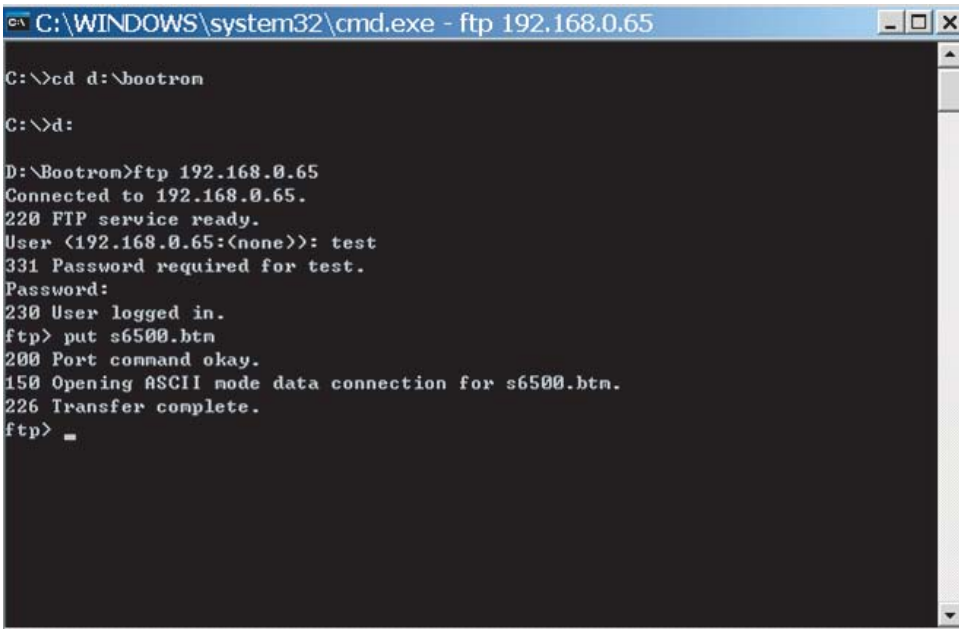
Step 6: Enter "ftp 192.168.0.65" and enter the user name test, password pass, as shown in Figure 226, to log on the FTP server.

Figure 226 Log on the FTP server



Step 7: Use the **put** command to upload the file s7500.btm to the switch, as shown in Figure 227.

Figure 227 Upload file s7500.btm to the switch



Step 8: Configure s7500.btm to be the BootROM at reboot, and then restart the switch.

```
<SW7750> boot bootrom s7500.btm slot 0
This will update BootRom file on board 0 . Continue? [Y/N] y
 Board 0 upgrading BOOTROM, please wait...
 Upgrade board 0 BOOTROM succeeded!
<SW7750> reboot
```

When rebooting the switch, use the file s7500.btm as BootROM to finish BootROM loading.

2 Loading host software

Loading the host software is the same as loading the BootROM program, except for that the file to be downloaded is the host software file, and that you need to use the **boot boot-loader** command to select the host software at reboot of the switch.

- *The steps listed above are performed in the Windows operating system, if you use other FTP client software, refer to the corresponding user's guide before operation.*
- *Only the configurations steps concerning loading are illustrated here, for detailed description on the corresponding configuration commands, refer to "FTP and TFTP Configuration" on page 803.*

Remote Loading Using TFTP

The remote loading using TFTP is similar to that using FTP. The only difference is that TFTP is used instead off FTP to load software to the switch, and the switch can only act as a TFTP client.

CAUTION:

- *Fabric software and I/O Module (line processing unit) software must be identical. Otherwise the Switch 7750 cannot work normally.*
- *To keep the software of Fabric and I/O Module identical, you need to restart the I/O Module after you upgrade the host software of the Fabric of the Switch 7750 Ethernet switches.*
- *The Switch 7758 features the double Fabrics and active-standby switchover function. If a switch possesses two Fabrics, with the active-standby switchover function enabled, you can in turn upgrade and restart the two Fabrics with one Fabric being active. Although Fabric can be upgraded through hot backup, because the I/O Module must be restarted to keep identical with the Fabric's software, your services will still be interrupted during the I/O Module restart period. Therefore, you are recommended to restart the whole switch straight after you upgrade the host software of the Fabric of the Switch 7758.*

78 BASIC SYSTEM CONFIGURATION & DEBUGGING

Basic System Configuration

Basic System Configuration Tasks

Table 659 Basic system configuration tasks

Operation	Description	Related section
Enter system view from user view	-	"Entering System View from User View" on page 853
Set the system name of the switch	Optional	"Setting the System Name of the Switch" on page 853
Set the date and time of the system	Optional	"Setting the Date and Time of the System" on page 854
Set the local time zone	Optional	"Setting the Local Time Zone" on page 854
Set the summer time	Optional	"Setting the Summer Time" on page 854
Set the CLI language mode	Optional	"Setting the CLI Language Mode" on page 854
Return from current view to lower level view	-	"Returning from Current View to Lower Level View" on page 855
Return from current view to user view	-	"Returning from Current View to User View" on page 855

Entering System View from User View

Table 660 Enter system view from user view

Operation	Command	Description
Enter system view from user view	**system-view**	-

Setting the System Name of the Switch

Table 661 Set the system name of the switch

Operation	Command	Description
Enter system view	**system-view**	-
Set the system name of the switch	**sysname** *sysname*	Optional By default, the name is 3Com.

Setting the Date and Time of the System

Table 662 Set the date and time of the system

Operation	Command	Description
Set the current date and time of the system	**clock datetime** *HH:MM:SS YYYY/MM/DD*	Optional

Setting the Local Time Zone

This configuration task is to set the name of the local time zone and the difference between the local time zone and the standard UTC (universal time coordinated) time.

Table 663 Set the local time zone

Operation	Command	Description
Set the local time zone	**clock timezone** *zone-name* { **add** | **minus** } *HH:MM:SS*	Optional By default, it is the UTC time zone.

Setting the Summer Time

This configuration task is to set the name, time range (start time and end time), and time offset of the summer timer. The operation here saves you from manually adjust the system time.

- When the system reaches the specified start time, it automatically adds the specified offset to the current time, so as to toggle the system time to the summer time.
- When the system reaches the specified end time, it automatically subtracts the specified offset from the current time, so as to toggle the summer time to normal system time.

Perform the following configuration in user view.

Table 664 Set the summer time

Operation	Command	Description
Set the name and time range of the summer time	**clock summer-time** *zone-name* **one-off** *start-time start-date end-time end-date offset-time* **clock summer-time** *zone-name* **repeating** { *start-time start-date end-time end-date* | *start-time start-year start-month start-week start-day end-time end-year end-month end-week end-day* } *offset-time*	Optional

Setting the CLI Language Mode

Table 665 Set the CLI language mode

Operation	Command	Description
Set the CLI language mode	**language-mode** { **chinese** | **english** }	Optional By default, the command line interface (CLI) language mode is English.

Returning from Current View to Lower Level View

Table 666 Return from current view to lower level view

Operation	Command	Description
Return from current view to lower level view	**quit**	This operation will result in exiting the system if current view is user view.

Returning from Current View to User View

Table 667 Return from current view to user view

Operation	Command	Description
Return from current view to user view	**return**	The composite key <Ctrl+Z> has the same effect with the **return** command.

Displaying the System Status

You can use the following **display** commands to check the status and configuration information about the system. For information about protocols and ports, and the associated **display** commands, refer to relevant sections.

Table 668 System display commands

Operation	Command	Description
Display the current date and time of the system	**display clock**	You can execute the **display** command in any view
Display the version of the system	**display version**	
Display the information about user terminal interfaces	**display users** [**all**]	
Display the debugging status	**display debugging** [**interface** *interface-type interface-number*] [*module-name*]	

System Debugging

Enabling/Disabling System Debugging

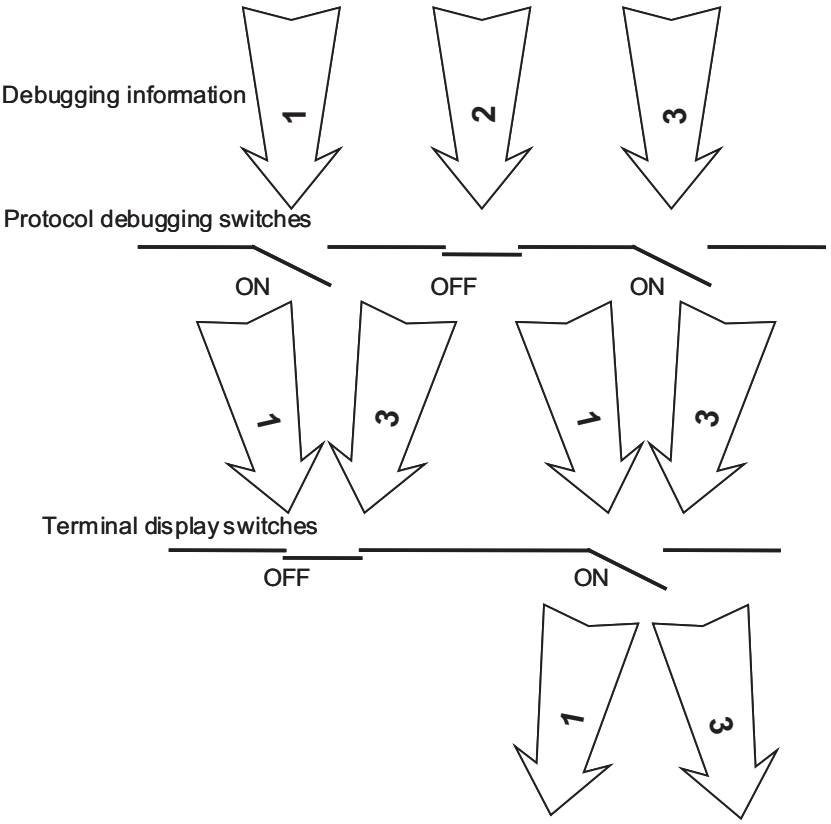
The Ethernet switch provides a variety of debugging functions. Most of the protocols and features supported by the Ethernet switch are provided with corresponding debugging functions. These debugging functions are a great help for you to diagnose and troubleshoot your switch system.

The output of debugging information is controlled by two kinds of switches:

- Protocol debugging, which controls whether the debugging information of a protocol is output.
- Terminal display, which controls whether the debugging information is output to a user screen.

The relation between the two switches is as follows:

Figure 228 Debugging information output



You can use the following commands to operate the two kinds of switches.

Perform the following operations in user view.

Table 669 Enable debugging and terminal display

Operation	Command	Description
Enable system debugging	**debugging** { **all** [**timeout** *interval*] | *module-name debugging-option* }	By default, all debugging is disabled in the system. Because the output of debugging information will affect the efficiency of the system, disable your debugging after you finish it.
Enable terminal display for debugging	**terminal debugging**	By default, terminal display for debugging is disabled.

Displaying Debugging Status

Table 670 Display the current debugging status in the system

Operation	Command	Description
Display all enabled debugging on the specified device	**display debugging** [**interface** *interface-type interface-number*] [*module-name*]	You can execute the **display** command in any view.

Displaying Operating Information about Modules in System

When your Ethernet switch is in trouble, you may need to view a lot of operating information to locate the problem. Each functional module has its own operating information display command(s). You can use the command here to display the current operating information about the modules (settled when this command is designed) in the system for troubleshooting your system.

Perform the following operation in any view.

Table 671 Display the current operation information about the modules in the system.

Operation	Command	Description
Display the current operation information about the modules in the system.	**display diagnostic-information** [*module-name*]	You can execute this command twice and find the difference between the two executing results to locate the problem.

79 NETWORK CONNECTIVITY TEST

Network Connectivity Test

ping

You can use the **ping** command to check the network connectivity and the reachability of a host.

Table 672 The ping command

Operation	Command
Support IP protocol	**ping** [**-a** *ip-address* | **-c** *count* | **-d** | **-f** | **-h** *ttl* | **-i** *interface-type interface-number* | **-n** | **- p** *pattern* | **-q** | **-r** | **-s** *packetsize* | **-t** *timeout* | **-tos** *tos* | **-v** | **ip**]* *host-ip*
Support IPX protocol	**ping ipx** *ipx-address* [**-c** *count* | **-s** *packetsize* | **-t** *timeout*]*
Support CLNS protocol	**ping clns** *nsap-address*

This command can output the following results:

- Response status for each ping packet. If no response packet is received within the timeout time, the message "Request time out" is displayed. Otherwise, the number of data bytes, packet serial number, TTL (time to live) and response time of the response packet are displayed.
- Final statistics, including the numbers of sent packets and received response packets, the unresponsive packet percentage, and the minimum, average and maximum values of response time.

tracert

You can use the **tracert** command to trace the gateways a packet passes during its journey from the source to the destination. This command is mainly used to check the network connectivity. It can help you locate the trouble spot of the network.

The executing procedure of the **tracert** command is as follows: First, the source host sends a data packet with the TTL of 1, and the first hop device returns an ICMP error message indicating that it cannot forward this packet because of TTL timeout. Then, the source host resends the packet with the TTL of 2, and the second hop device also returns an ICMP TTL timeout message. This procedure goes on and on until the packet gets to the destination. During the procedure, the system records the source address of each ICMP TTL timeout message in order to offer the path that the packet passed through to the destination.

Table 673 The tracert command

Operation	Command
Support IP protocol	**tracert** [**-a** *source-ip* | **-f** *first-TTL* | **-m** *max-TTL* | **-p** *port* | **-q** *num-packet* | **-w** *timeout*] * *host*
Support CLNS protocol	**tracert clns** [**-m** *max-TTL* | **-n** *num-packet* | **-t** *timeout* | **-v**]* *nsap-address*

80 DEVICE MANAGEMENT

When different switch fabrics work together with a chassis, note that:

If the 96Gbps Switch Fabric switch works with the Switch 7708 chassis without the XGbus silkscreen, the four SFP interfaces on the switch fabric do not work.

If a 96Gbps Switch Fabric is installed in a Switch 7758 XGbus chassis, the four SFP interfaces on the switch fabric all work normally.

When two 96Gbps Switch Fabrics are installed into the Switch 7758 XGbus chassis,

- *The first two SFP interfaces of the primary module and the first two SFP interfaces of the secondary module work normally. Services will not be interrupted during active-standby switchover.*
- *The last two SFP interfaces on the primary module and the last two interfaces on the secondary module do not work, and you can not see these four interfaces through command line interface.*
- *When the secondary module is inserted, configurations on the last two SFP interfaces of the primary module will not be sent to the first two SFP interfaces of the secondary module automatically, and you need to do this manually.*

Introduction to Device Management

The device management function of the Ethernet switch can report the current status and event-debugging information of the modules to you. Through this function, you can maintain and manage your physical device, and restart the system when some functions of the system are abnormal.

Device Management Configuration

Device Management Configuration Tasks

Table 674 Device management configuration tasks

Operation	Description	Related section
Restart the Ethernet switch	-	"Restarting the Ethernet Switch" on page 862
Reboot a module of Ethernet switch	Optional	"Rebooting a Module of Ethernet Switch" on page 862
Schedule a reboot on the switch	Optional	"Scheduling a Reboot on the Switch" on page 862
Specify the ARP to be adopted at reboot	Optional	"Specifying the APP to be Adopted at Reboot" on page 863

Table 674 Device management configuration tasks

Operation	Description	Related section
Update the BootROM	Optional	"Updating the BootROM" on page 863
Upgrade BootROM along with the upgrade of ARP	Optional	"Upgrading BootROM along with the Upgrade of ARP" on page 863
Set module temperature threshold	Optional	"Setting Module Temperature Threshold" on page 864
Enable/disable RDRAM	Optional	"Enabling/Disabling RDRAM" on page 864
Enable system load sharing	Optional	"Enabling System Load Sharing" on page 864
Identifying and Diagnosing Pluggable Transceivers	Optional	"Identifying and Diagnosing Pluggable Transceivers" on page 865

Restarting the Ethernet Switch

You can perform the following operation in user view when the switch is in trouble or needs to be restarted.

Table 675 Restart the Ethernet switch

Operation	Command	Description
Restart the Ethernet switch	**reboot**	-

When rebooting, the system checks whether there is any configuration change. If there is, it prompts you to indicate whether or not to proceed. This prevents you from losing your original configuration due to oblivion after system reboot.

Rebooting a Module of Ethernet Switch

It would be necessary to reset a module of Ethernet switch when failure occurs.

Table 676 Reset a card

Operation	Command	Description
Reset a module of Ethernet switch	**reboot** [**slot** *slot-number*]	Optional

The value of *slot-number* ranges with products:

- Switch 7754: 0 to 3
- Switch 7757: 0 to 6
- Switch 7758: 0 to 7

The value 0 indicates to reset the Fabric, equivalent to resetting the switch system.

Scheduling a Reboot on the Switch

After you schedule a reboot on the switch, the switch will reboot at the specified time.

Table 677 Schedule a reboot on the switch

Operation	Command	Description
Schedule a reboot on the switch, and set the reboot date and time	**schedule reboot at** *hh:mm* [*yyyy/mm/dd*]	Optional

Table 677 Schedule a reboot on the switch

Operation	Command	Description
Schedule a reboot on the switch, and set the reboot waiting delay	**schedule reboot delay** { *hhh:mm* | *mmm* }	Optional



There is at most one minute defer for scheduled reboot, that is, the switch will reboot within one minute after reaching the specified reboot date and time.

Specifying the APP to be Adopted at Reboot

APP is the host software of the switch. If multiple APPs exist in the Flash memory, you can use the command here to specify the one that will be adopted when the switch reboots.

The Switch 7750 Ethernet switches feature double Fabrics. When both the active and standby Fabrics need to be upgraded, you need to specify the APP file used for the next startup for the active Fabric and the standby Fabric respectively. Note that, you must specify the APP file for the active Fabric from the Flash or CF module of the active Fabric, and that for the standby Fabric from the Flash or CF module of the standby Fabric.

Perform the following configuration in user view:

Table 678 Specify the APP to be adopted at reboot

Operation	Command	Description
Specify the APP to be adopted at reboot	**boot boot-loader** { **primary** | **backup** } *file-url*	Optional

Updating the BootROM

You can use the BootROM application saved in the Flash memory of the switch to update the running BootROM application. With this command, a remote user can conveniently update the BootRom by uploading the BootROM to the switch through FTP and running this command. The BootROM can be used when the switch reboots.

Perform the following configuration in user view:

Table 679 Update the BootROM

Operation	Command	Description
Update the BootROM	**boot bootrom** *file-url* **slot** *slot-list*	Optional

Upgrading BootROM along with the Upgrade of ARP

Upgrading BootROM along with ARP can ensure the best matching between the version of current primary module and the version of BootROM, so as to avoid the mal-operations of some functions and features caused by unmatched versions.

This feature supports two upgrade types:

- Use the current boot file as the upgrade file of BootROM.
- Specify the ARP file as the upgrade file of BootROM.

Table 680 Configure to upgrade BootROM

Operation	Command	Description
Use the current boot file to upgrade BootROM	**boot bootrom default** [**slot** *slot-list*]	Optional

CAUTION:

- *If you do not specify the slot number to upgrade in the boot bootrom command, the system will upgrade all the modules working normally by default.*
- *After you specify the boot file of the primary module, if you want to upgrade BootROM, the system will upgrade all modules working normally by default. During the upgrade process, the system will prompt you to confirm whether to upgrade or not.*

Setting Module Temperature Threshold

The switch system alarms when the temperature on a module exceeds a specified temperature range.

Table 681 Set module temperature threshold

Operation	Command	Description
Set module temperature threshold	**temperature-limit** *slot-number down-value up-value*	Optional

Enabling/Disabling RDRAM

Using the following command, yon can enable or disable RDRAM (Rambus Dynamic Random Access Memory) of the device.

Table 682 Enable/Disable RDRAM

Operation	Command	Description
Enter system view	**system-view**	-
Enable RDRAM of the device	**rdram enable**	Optional
Disable RDRAM of the device	**rdram disable**	By default, RDRAM is disabled.

Enabling System Load Sharing

With system load sharing enabled, after an I/O Module receives traffic to be cross-card forwarded, load sharing is performed between the active Fabric and the standby Fabric.

Table 683 Enable system load sharing

Operation	Command	Description
Enter system view	**system-view**	-
Enable system load sharing function	**loadsharing enable**	Required By default, system load sharing is disabled.

- *Only unicast traffic supports load sharing.*
- *The 96Gbps Switch Fabric and GEbus I/O Modules do not support load sharing.*
- *Only I/O Module of XGbus type supports load sharing.*

Identifying and Diagnosing Pluggable Transceivers

Introduction to pluggable transceivers

At present, four types of pluggable transceivers are commonly used, and they can be divided into optical transceivers and electrical transceivers based on transmission media as shown in Table 684.

Table 684 Commonly used pluggable transceivers

Transceiver type	Applied environment	Whether can be an optical transceiver	Whether can be an electrical transceiver
SFP (Small Form-factor Pluggable)	Generally used for 100M/1000M Ethernet interfaces or POS 155M/622M/2.5G interfaces	Yes	Yes
GBIC (GigaBit Interface Converter)	Generally used for 1000M Ethernet interfaces	Yes	Yes
XFP (10-Gigabit small Form-factor Pluggable)	Generally used for 10G Ethernet interfaces	Yes	No
XENPAK (10 Gigabit EtherNet Transceiver Package)	Generally used for 10G Ethernet interfaces	Yes	Yes

For pluggable transceivers supported by Switch 7750 Ethernet switches, refer to 3Com Switch 7750 Family Installation Manual.

Identifying pluggable transceivers

As pluggable transceivers are of various types and from different vendors, you can perform the following configurations to identify main parameters of the pluggable transceivers, including transceiver type, connector type, central wavelength of the laser sent, transfer distance and vendor name or vendor name specified.

Follow these steps to identify pluggable transceivers:

To do...	Use the command...	Remarks
Display main parameters of the pluggable transceiver(s)	**display transceiver interface** [*interface-type interface-number*]	Available for all pluggable transceivers
Display part of the electrical label information of the anti-spoofing transceiver(s) customized by 3Com	**display transceiver manuinfo interface** [*interface-type interface-number*]	Available for anti-spoofing pluggable transceiver(s) customized by 3Com only

- You can use the **Vendor Name** field in the prompt information of the **display transceiver interface** command to identify an anti-spoofing pluggable transceiver customized by 3Com. If the field is **3Com**, it is considered an 3Com-customized pluggable transceiver.
- Electrical label information is also called permanent configuration data or archive information, which is written to the storage device of a module during device debugging or test. The information includes name of the module, device serial number, and vendor name or vendor name specified.

Diagnosing pluggable transceivers

The system outputs alarm information for you to diagnose and troubleshoot faults of pluggable transceivers. Optical transceivers customized by 3Com also support the digital diagnosis function, which enables a transceiver to monitor the main parameters such as temperature, voltage, laser bias current, TX power, and RX power. When these parameters are abnormal, you can take corresponding measures to prevent transceiver faults.

Follow these steps to display pluggable transceiver information:

To do...	Use the command...	Remarks
Display the current alarm information of the pluggable transceiver(s)	**display transceiver alarm interface** [*interface-type interface-number*]	Available for all pluggable transceivers
Display the currently measured value of the digital diagnosis parameters of the anti-spoofing optical transceiver(s) customized by 3Com	**display transceiver diagnosis interface** [*interface-type interface-number*]	Available for anti-spoofing pluggable optical transceiver(s) customized by 3Com only

Configuring Pause Frame Protection Mechanism

Pause frames, which can be utilized as packets to attack a network, are used in traffic controlling. A switch that has pause frame protection mechanism enabled discards the detected pause frames that are utilized to attack the network it resides and logs these attacks in the logbuffer. If the switch experiences successive pause frame attacks, it sends messages to the console to warn users.



CAUTION: *Only A type modules support pause frame protection mechanism and the related commands. A type modules include: 3C16860, 3C16861, LS81FS24A, 3C16858, and 3C16859.*

Pause Frame Protection Mechanism Configuration Task

The following describes the configuration tasks of Pause Frame protection mechanism.

Table 685 Configure pause frame protection mechanism

Operation	Command	Description
Enter system view	**system-view**	-
Enable pause frame protection mechanism	**pause-protection enable slot** *slot-number*	Required Pause frame protection mechanism is disabled by default.

Pause Frame Protection Mechanism Configuration Example

Network requirements

Enable pause frame protection mechanism on the module in Slot 7 of the switch.

Configuration procedure

1 Enter system view.

```
<SW7750> system-view
[SW7750]
```

2 Enable pause frame protection mechanism on the module seated in slot 7.

```
[SW7750] pause-protection enable slot 7
```

Configuring Layer 3 Connectivity Detection

Introduction to layer 3 connectivity detection

The function that detects layer 3 connectivity is implemented as follows. Local devices send ARP request packets continuously to the IP addresses of the devices to be detected. Users can then locate, solve, and log link problems by monitoring the peer devices through the received ARP response packets.



This function requires no Layer 3 device existing between the local peer and the remote peer.

Layer 3 Connectivity Detection Configuration Task



Before performing this configuration, make sure the physical link between the local peer and the remote peer is correct, and the related VLAN interfaces are assigned with correct IP addresses.

Table 686 Configure Layer 3 connectivity detection

Operation	Command	Description
Enter system view	**system-view**	-
Enter Ethernet interface view	**interface** *interface-type interface-number*	-
Enable Layer 3 connectivity detection function	**uplink monitor ip** *ip-address*	Required
Display information about Layer 3 connectivity between the local device and the remote device.	**display uplink monitor**	Optional You can execute the **display** command in any view.

Layer 3 Connectivity Detection Configuration Example

Network requirements

- The physical link between the local peer and the remote peer is correct. The local peer port that is used to connect is Ethernet4/0/1.
- The IP address of the lay 3 interface of the remote peer is 1.1.1.1.

Configuration procedure

Enter system view.

```
<SW7750> system-view
[SW7750]
```

Enter Ethernet interface view.

```
[SW7750] interface Ethernet 4/0/1
```

Enable Layer 3 connectivity detection on Ethernet4/0/1 interface and specify the IP address of the device (1.1.1.1) to be detected.

```
[SW7750-Ethernet4/0/1] uplink monitor ip 1.1.1.1
```

Configuring Queue Traffic Monitoring

Upon enabling queue traffic monitoring on a switch, the switch monitors the queue traffic and relieves blocks in the output queue of its interfaces.

The criterion used to distinguish a block is that the queue is full, and the traffic of the corresponding interface is less than the specified threshold.

Queue Traffic Monitoring Configuration Task

The following describes configuration tasks of queue traffic monitoring.

Table 687 Configure queue traffic monitoring

Operation	Command	Description
Enter system view	**system-view**	-
Enable queue traffic monitoring	**qe monitor enable**	Required This function is enabled by default.
Set the overall traffic threshold	**qe monitor overflow-threshold** *threshold*	Optional 300,000,000 bps by default.

Queue Traffic Monitoring Configuration Example

Network requirements

- Enable queue traffic monitoring.
- Set the overall traffic threshold used in queue traffic monitoring to 90 Mbps.

Configuration procedure

Enter system view.

```
<SW7750> system-view
[SW7750]
```

Enable queue traffic monitoring.

```
[SW7750] qe monitor enable
```

Set the overall traffic threshold used in queue traffic monitoring to 90 Mbps.

```
[SW7750] qe monitor overflow-threshold 90000000
```

Configuring Error Packets Monitoring

If the switch receives a great number of error packets, it will not be able to send/receive packets properly. With error packets monitoring enabled, the switch collects information about received error packets regularly. If error packets are detected, it takes protection measures to ensure that its interfaces send/receive packets properly.

Error Packets Monitoring Configuration Task

The following describes configuration tasks of error packets monitoring.

Table 688 Configure error packets monitoring

Operation	Command	Description
Enter the system view	**system-view**	-
Set the interval for detecting error packets	**qe monitor errpkt check-time** *interval*	Optional Defaults to 5 seconds.
Enter Ethernet interface view	**interface** *interface-type interface-number*	-
Enable error packets monitoring	**qe monitor errpkt** { **all** | **none** | **runt** }	Required. If you specify the keyword all in the command, the switch detects all error packets on current interface. If you specify the keyword runt, the switch only detects error packets that are of runt type on current interface. If you specify the keyword none, the switch does not detect the error packets on current interface.

Error Packets Monitoring Configuration Example

Network requirements

- Enable error packets monitoring on Ethernet4/0/1 interface and only the packets that are of runt type are concerned.
- Set the interval for detecting error packets to 50 seconds.

Configuration procedure

Enter system view.

```
<SW7750> system-view
[SW7750]
```

Set the interval for detecting error packets to 50 seconds.

```
[SW7750] qe monitor errpkt check-time 50
```

Enter Ethernet interface view of Ethernet4/0/1.

```
[SW7750] interface Ethernet 4/0/1
[SW7750-Ethernet4/0/1]
```

Specify only detect current interface for error packets of runt type.

```
[SW7750-Ethernet4/0/1] qe monitor errpkt runt
```

Displaying the Device Management Configuration

After the above configurations, you can execute the **display** command in any view to display the operating status of the device management to verify the configuration effects.

Table 689 Display the operating status of the device management

Operation	Command	Description
Display the APP to be adopted at reboot	**display boot-loader**	You can execute the **display** command in any view.
Display the module type and operating status of each board	**display device** [**detail** | [**shelf** *shelf-no*] [**frame** *frame-no*] [**slot** *slot-number*]]	
Display information about environment used by a switch	**display environment**	
Display the operating status of the built-in fan	**display fan** [*fan-id*]	
Display the usage of s switch	**display cpu** [**slot** *slot-number*]	
Display memory usage of a switch	**display memory** [**slot** *slot-number* | **limit**]	
Display the operating status of the power supply	**display power** [*power-id*]	

Remote Switch Update Configuration Example

Network requirements

Telnet to the switch from a PC remotely and download applications from the FTP server to the Flash memory of the switch to remotely update the switch software by using the device management commands through CLI.

The switch acts as the FTP client, and the remote PC serves as both the configuration PC and the FTP server.

Perform the following configuration on the FTP server.

- Configure an FTP user, whose name and password are switch and hello respectively. Authorize the user with the read-write right of the Switch directory on the PC.
- Make appropriate configuration so that the IP address of a VLAN interface on the switch is 1.1.1.1, the IP address of the PC is 2.2.2.2, and the switch and the PC is reachable to each other.

The host software switch.app and the BootROM file boot.btm of the switch are stored into the directory of the switch. Use FTP to download the switch.app and boot.btm files from the FTP server to the switch.

Network diagram

Figure 229 Network diagram of FTP configuration



Configuration procedure

1 Configure the following FTP server-related parameters on the PC: an FTP user with the username and password as switch and hello respectively, and specify the

working directory of the user as Switch. The detailed configuration is omitted here.

2 Configure the switch as follows:

On the switch, configure a level 3 telnet user with the username and password as user and hello respectively. Authentication by user name and password is required for the user.



Refer to "Controlling Telnet Users" on page 77.

Execute the **telnet** command on the PC to log into the switch. The following prompt appears:

```
<SW7750>
```



CAUTION: *If the Flash memory of the switch is not sufficient, delete the original applications in it before downloading the new ones.*

Initiate an FTP connection with the following command in user view. Input the correct user name and password to log into the FTP server.

```
<SW7750> ftp 2.2.2.2
Trying ...
Press CTRL+K to abort
Connected.
220 FTP service ready.
User(none):switch
331 Password required for switch.
Password:
230 User logged in.
[ftp]
```

Execute the **get** command to download the switch.app and boot.btm files on the FTP server to the Flash memory of the switch.

```
[ftp] get switch.app
[ftp] get boot.btm
```

Execute the **quit** command to terminate the FTP connection and return to user view.

```
[ftp] quit
<SW7750>
```

Update the BootROM.

```
<SW7750> boot bootrom boot.btm slot 0
This will update BootRom file on board 0 . Continue? [Y/N] y
 Board 0 upgrading BOOTROM, please wait...
 Upgrade board 0 BOOTROM succeeded!
```

Specify the downloaded application program as the host software to be adopted when the switch starts next time. Then restart the switch to update the host software of the switch.

```
<SW7750> boot boot-loader primary switch.app
 The specified file will be booted next time on unit 1!
<SW7750> display boot-loader
The primary app to boot of board 0 at the next time is: flash:/switch.app
 The backup app to boot of board 0 at the next time is: flash:/old.app
 The app to boot of board 0 at this time is: flash:/old.app
<SW7750> reboot
```

81 REMOTE-PING CONFIGURATION

Remote-ping Overview

Introduction to Remote-ping

Remote-ping is a network diagnostic tool. It is used to test the performance of various protocols running in networks. Remote-ping provides more functions than the **ping** command.

- The **ping** command can only use the ICMP protocol to test the round trip time (RTT) between this end and a specified destination end for the user to judge whether the destination end is reachable.
- Besides the above function of the **ping** command, remote-ping can also provide other functions, such as testing the status (open/close) of a DHCP/FTP/HTTP/SNMP server and the response time of various services.

You need to configure the remote-ping client and sometimes the corresponding remote-ping servers to perform various remote-ping tests. All remote-ping tests are initiated by the remote-ping client and you can view the test results on remote-ping client only.

When performing a remote-ping test, you need to configure a remote-ping test group on the remote-ping client. A remote-ping test group is a set of remote-ping test parameters. A test group contains several test parameters and is uniquely identified by an administrator name and a test tag.

After creating a remote-ping test group and configuring the test parameters, you can then perform a remote-ping test by the **test-enable** command.

- Being different from the **ping** command, remote-ping does not display the RTT or timeout status of each packet on the Console terminal in real time. To view the statistic results of your remote-ping test operation, you need to execute the **display remote-ping** command.
- Remote-ping also allows you to set parameters for remote-ping test groups, start remote-ping tests and view statistical test results through a network management device.

Figure 230 Remote-ping illustration



Test Types Supported by Remote-ping

Among the test types supported by remote-ping, only the ICMP test can be performed when IRF fabric is enabled; all other test types cannot be performed when IRF fabric is enabled.

Table 690 Test types supported by remote-ping

Supported test types		Description
ICMP test		For these types of tests, you need to configure the remote-ping client and the corresponding servers.
DHCP test		
FTP test		
HTTP test		
DNS test		
SNMP test		
Jitter test		■ These types of tests need the cooperation of the remote-ping client and remote-ping server. ■ Do not perform a TCP, UDP or jitter test on a well-known port (ports with a number ranging from 1 to 1023) or on a port with a port number greater than 50000. Otherwise, your remote-ping test may fail or the service corresponding to the well-known port may become unavailable.
TCP test	Tcppublic test	
	Tcpprivate test	
UDP test	Udppublic test	
	Udpprivate test	

Remote-ping Test Parameters

You need to configure corresponding test parameters for each type of remote-ping test. remote-ping test parameters can be configured on remote-ping client only. For the configurations on remote-ping client, refer to "Remote-ping Client Configuration" on page 877.

Table 691 Remote-ping test parameters

Test parameter	Description
Destination address (**destination-ip**)	For TCP/UDP/jitter test, you must specify a destination IP address, and the destination address must be the IP address of a TCP/UDP/UDP listening service configured on the remote-ping server.
Destination port (**destination-port**)	For tcpprivate/udpprivate/jitter test, you must specify a destination port number, and the destination port number must be the port number of a TCP or UDP listening service configured on the remote-ping server.
Source interface (**source-interface**)	■ For DHCP test, you must specify a source interface, which will be used by remote-ping client to send DHCP requests. If no source interface is specified for a DHCP test, the test will not succeed. ■ After a source interface is specified, remote-ping client uses this source interface to send DHCP requests during a DHCP test. ■ The IP address of the specified source interface will be used as the source IP address of DHCP requests.

Table 691 Remote-ping test parameters

Test parameter	Description
Source address (**source-ip**)	For remote-ping tests other than DHCP test, you can specify a source IP address for test packets, which will be used by the server as the destination address of response packets.
Source port (**source-port**)	For remote-ping tests other than ICMP, DHCP and DNS, you can specify a source port number for test packets, which will be used by the server as the destination port number of response packets.
Test type (**test-type**)	■ You can use remote-ping to test a variety of protocols, see Table 690 for details. ■ To perform a type of test, you must first create a test group of this type. One test group can be of only one remote-ping test type. ■ If you modify the test type of a test group using the **test-type** command, the parameter settings, test results, and history records of the original test type are all cleared.
Number of probes per test (**count**)	■ For tests except jitter test, only one test packet is sent in a probe. In a jitter test, you can use the **jitter-packetnum** command to set the number of packets to be sent in a probe.
Packet size (**datasize**)	■ For ICMP/UDP/jitter test, you can configure the size of test packets. ■ For ICMP test, the ICMP packet size refers to the length of ECHO-REQUEST packets (excluding IP and ICMP headers)
Maximum number of history records that can be saved (**history-records**)	This parameter is used to specify the maximum number of history records that can be saved in a test group. When the number of saved history records exceeds the maximum number, remote-ping discards some earliest records.
Automatic test interval (**frequency**)	This parameter is used to set the interval at which the remote-ping client periodically performs the same test automatically.
Probe timeout time (**timeout**)	■ The probe timeout timer is started after the remote-ping client sends out a test packet. ■ This parameter is in seconds.
Type of service (**tos**)	Type of service is the value of the ToS field in IP header in the test packets.
dns	This parameter is used to specify a DNS domain name in a remote-ping DNS test group.
dns-server	This parameter is used to set the DNS server IP address in a remote-ping DNS test group.
HTTP operation type (**http-operation**)	This parameter is used to set the type of HTTP interaction operation between remote-ping client and HTTP server.

Table 691 Remote-ping test parameters

Test parameter	Description
HTTP operation string and version (**http-string**)	This parameter is used to set the HTTP operation string and version in an HTTP test.
FTP operation type (**ftp-operation**)	This parameter is used to set the type of FTP interaction operation between remote-ping client and FTP server.
FTP operation type (**ftp-operation**)	This parameter is used to set the type of FTP interaction operation between remote-ping client and FTP server.
FTP login username and password (**username** and **password**)	The two parameters are used to set the username and password to be used for FTP operation.
File name for FTP operation (**filename**)	Name of a file to be transferred between remote-ping client and FTP server
Number of jitter test packets to be sent per probe (**jitter-packetnum**)	■ Jitter test is used to collect statistics about delay jitter in UDP packet transmission ■ In a jitter probe, the remote-ping client sends a series of packets to the remote-ping server at regular intervals (you can set the interval). Once receiving such a packet, the remote-ping server marks it with a timestamp, and then sends it back to the remote-ping client. Upon receiving a packet returned, the remote-ping client computes the delay jitter time. The remote-ping client collects delay jitter statistics on all the packets returned in the test. So, the more packets a jitter probe sends, the more accurate the jitter statistics is, but the longer time the jitter test costs.
Interval to send jitter test packets (**jitter-interval**)	Each jitter probe will send multiple UDP test packets at regular intervals (you can set the interval). The smaller the interval is, the faster the test is. But a too small interval may somewhat impact your network.
Trap	■ A remote-ping test will generate a Trap message no matter whether the test successes or not. You can use the Trap switch to enable or disable the output of trap messages. ■ You can set the number of consecutive failed remote-ping tests before Trap output. You can also set the number of consecutive failed remote-ping probes before Trap output.

Remote-ping Configuration

The TCP/UDP/jitter tests need the cooperation of remote-ping client and remote-ping Server, Other types of tests need to configure remote-ping client and corresponding different servers.

Configuration on a Remote-ping Server

You can enable both the remote-ping client and remote-ping server functions on a Switch 7750, that is, the switch can serve as a remote-ping client and server simultaneously.

Remote-ping server configuration tasks

Table 692 Remote-ping server configuration tasks

Item	Description	Related section
Enable the remote-ping server function	The remote-ping server function is needed only for jitter, TCP, and UDP tests.	"Remote-ping server configuration"
Configure a listening service on the remote-ping server	You can configure multiple TCP/UDP listening services on one remote-ping server, with each listening service corresponding to a specific destination IP address and port number.	"Remote-ping server configuration"

Remote-ping server configuration

Table 693 describes the configuration on remote-ping server, which is the same for remote-ping test types that need to configure remote-ping server.

Table 693 Remote-ping server configuration

Operation	Command	Description
Enter system view	**system-view**	-
Enable the remote-ping server function	**remote-ping-server enable**	Required Disabled by default.
Configure a UDP listening service	**remote-ping-server udpecho** *ip-address port-num*	Required for UDP and jitter tests By default, no UDP listening service is configured.
Configure a TCP listening service	**remote-ping-server tcpconnect** *ip-address port-num*	Required for TCP tests By default, no TCP listening service is configured.

- The remote-ping server function is needed only for jitter, TCP, and UDP tests.
- You can configure multiple TCP/UDP listening services on one remote-ping server, with each listening service corresponding to a specific destination IP address and port number.

Remote-ping Client Configuration

Remote-ping client configuration

After remote-ping client is enabled, you can create multiple test groups for different tests, without the need to enable remote-ping client repeatedly for each test group.

Different types of remote-ping tests are somewhat different in parameters and parameter ranges. The following text describes the configuration on remote-ping client for different test types.

Among the test types supported by remote-ping, only the ICMP test can be performed when IRF fabric is enabled; all other test types cannot be performed when IRF fabric is enabled. With IRF fabric enabled, you are allowed to configure remote-ping tests and use the ***display*** *commands to check your configurations,*

but for non ICMP tests, the remote-ping tests you configured cannot be executed until fabric is disabled.

1 Configuring an ICMP test on remote-ping client

Table 694 Configure ICMP test on remote-ping client

Operation	Command	Description
Enter system view	**system-view**	-
Enable the remote-ping client function	**remote-ping-agent enable**	Required By default, the remote-ping client function is disabled.
Create a remote-ping test group and enter its view	**remote-ping** *administrator-name operation-tag*	Required By default, no test group is configured.
Configure the test type	**test-type icmp**	Optional By default, the test type is ICMP.
Configure the destination IP address	**destination-ip** *ip-address*	Required By default, no destination address is configured.
Configure the source IP address	**source-ip** *ip-address*	Optional By default, no source IP address is configured.
Configure the test type	**test-type icmp**	Optional By default, the test type is ICMP.
Configure the number of probes per test	**count** *times*	Optional By default, each test makes one probe.
Configure the packet size	**datasize** *size*	Optional By default, the packet size is 56 bytes.
Configure the maximum number of history records that can be saved	**history-records** *number*	Optional By default, the maximum number is 50.
Configure the automatic test interval	**frequency** *interval*	Optional By default, the automatic test interval is zero seconds, indicating no automatic test will be made.
Configure the probe timeout time	**timeout** *time*	Optional By default, a probe times out in three seconds.
Configure the type of service (ToS)	**tos** *value*	Optional By default, the service type is zero.
Start the test	**test-enable**	Required
Display test results	**display remote-ping results** [*admin-name operation-tag*]	Required Available in any view.

2 Configuring a DHCP test on remote-ping client

Table 695 Configure DHCP test on remote-ping client

Operation	Command	Description
Enter system view	**system-view**	-
Enable the remote-ping client function	**remote-ping-agent enable**	Required By default, the remote-ping client function is disabled.
Create a remote-ping test group and enter its view	**remote-ping** *administrator-name operation-tag*	Required By default, no test group is configured.
Configure the source interface	**source-interface** *interface-type interface-number*	Required You can only configure a VLAN interface as the source interface. By default, no source interface is configured.
Configure the test type	**test-type dhcp**	Required By default, the test type is ICMP.
Configure the number of probes per test	**count** *times*	Optional By default, each test makes one probe.
Configure the maximum number of history records that can be saved	**history-records** *number*	**Figure 231** Optional By default, the maximum number is 50.
Configure the probe timeout time	**timeout** *time*	Optional By default, a probe times out in three seconds.
Start the test	**test-enable**	Required
Display test results	**display remote-ping results** [*admin-name operation-tag*]	Required You can execute the command in any view.

3 Configuring an FTP test on a remote-ping client

Table 696 Configure an FTP test on a remote-ping client

Operation	Command	Description
Enter system view	**system-view**	-
Enable the remote-ping client function	**remote-ping-agent enable**	Required By default, the remote-ping client function is disabled.
Create a remote-ping test group and enter its view	**remote-ping** *administrator-name operation-tag*	Required By default, no test group is configured.
Configure the test type	**test-type ftp**	Required By default, the test type is ICMP.
Configure the destination IP address	**destination-ip** *ip-address*	Required By default, no destination address is configured.

Table 696 Configure an FTP test on a remote-ping client

Operation	Command	Description
Configure the source IP address	**source-ip** *ip-address*	Required By default, no source IP address is configured.
Configure the source port	**source-port** *port-number*	Optional By default, no source port is configured.
Configure the number of probes per test	**count** *times*	Optional By default, each test makes one probe.
Configure the maximum number of history records that can be saved	**history-records** *number*	**Figure 232** Optional By default, the maximum number is 50.
Configure the automatic test interval	**frequency** *interval*	Optional By default, the automatic test interval is zero seconds, indicating no automatic test will be made.
Configure the probe timeout time	**timeout** *time*	Optional By default, a probe times out in three seconds.
Configure the type of service	**tos** *value*	Optional By default, the service type is zero.
Configure the type of FTP operation	**ftp-operation** { **get** | **put** }	Optional By default, the type of FTP operation is **get**, that is, the FTP operation will get a file from the FTP server.
Configure an FTP login username	**username** *name*	Required By default, neither username nor password is configured.
Configure an FTP login password	**password** *password*	
Configure a file name for the FTP operation	**filename** *file-name*	Required By default, no file name is configured for the FTP operation
Start the test	**test-enable**	Required
Display test results	**display remote-ping results** [*admin-name operation-tag*]	Required You can execute the command in any view.

4 Configuring an HTTP test on a remote-ping client

Table 697 Configure an HTTP test on a remote-ping client

Operation	Command	Description
Enter system view	**system-view**	-

Table 697 Configure an HTTP test on a remote-ping client

Operation	Command	Description
Enable the remote-ping client function	**remote-ping-agent enable**	Required By default, the remote-ping client function is disabled.
Create a remote-ping test group and enter its view	**remote-ping** *administrator-name operation-tag*	Required By default, no test group is configured.
Configure the destination IP address	**destination-ip** *ip-address*	Required You can configure an IP address or a host name. By default, no destination address is configured.
Configure the test type	**test-type http**	Required By default, the test type is ICMP.
Configure dns-server	**dns-server** *ip-address*	**Figure 233** Required when you use the destination-ip command to configure the destination address as the host name. **Figure 234** By default, no IP address of the DNS server is configured.
Configure the source IP address	**source-ip** *ip-address*	Optional By default, no source IP address is configured.
Configure the source port	**source-port** port-number	Optional By default, no source port is configured.
Configure the number of probes per test	**count** *times*	Optional By default, each test makes one probe.
Configure the maximum number of history records that can be saved	**history-records** *number*	**Figure 235** Optional By default, the maximum number is 50.
Configure the automatic test interval	**frequency** *interval*	Optional By default, the automatic test interval is zero seconds, indicating no automatic test will be made.
Configure the probe timeout time	**timeout** *time*	Optional By default, a probe times out in three seconds.
Configure the type of service	**tos** *value*	Optional By default, the service type is zero.

Table 697 Configure an HTTP test on a remote-ping client

Operation	Command	Description
Configure the type of HTTP operation	**http-operation** { **get** | **post** }	Optional By default, the type of HTTP operation is **get**, that is, the HTTP operation will get data from the HTTP server.
Configure the HTTP operation string and version in an HTTP test	**http-string** *string version*	Required By default, HTTP operation string and version are not configured.
Start the test	**test-enable**	Required
Display test results	**display remote-ping results** [*admin-name operation-tag*]	Required You can execute the command in any view.

5 Configuring jitter test on remote-ping client

Table 698 Configure jitter test on remote-ping client

Operation	Command	Description
Enter system view	**system-view**	-
Enable the remote-ping client function	**remote-ping-agent enable**	Required By default, the remote-ping client function is disabled.
Create a remote-ping test group and enter its view	**remote-ping** *administrator-name operation-tag*	Required By default, no test group is configured.
Configure the test type	**test-type jitter**	Required By default, the test type is ICMP.
Configure the destination IP address	**destination-ip** *ip-address*	Required The destination address must be the IP address of a UDP listening service on the remote-ping server. By default, no destination address is configured.
Configure the destination port	**destination-port** *Port-number*	Required The destination port must be the port of a UDP listening service on the remote-ping server. By default, no destination port is configured.
Configure the source IP address	**source-ip** *ip-address*	Optional By default, no source IP address is configured.
Configure the source port	**source-port** *port-number*	Optional By default, no source port is configured.

Table 698 Configure jitter test on remote-ping client

Operation	Command	Description
Configure the number of probes per test	**count** *times*	Optional By default, each test makes one probe.
Configure the maximum number of history records that can be saved	**history-records** *number*	**Figure 236** Optional By default, the maximum number is 50.
Configure the packet size	**datasize** *size*	Optional By default, the packet size is 68 bytes.
Configure the automatic test interval	**frequency** *interval*	Optional By default, the automatic test interval is zero seconds, indicating no automatic test will be made.
Configure the probe timeout time	**timeout** *time*	Optional By default, a probe times out in three seconds.
Configure the type of service	**tos** *value*	Optional By default, the service type is zero.
Configure the number of test packets that will be sent in each jitter probe	**jitter-packetnum** *number*	Optional By default, each jitter probe will send 10 packets.
Configure the interval to send test packets in the jitter test	**jitter-interval** *interval*	Optional By default, the interval is 20 milliseconds.
Start the test	**test-enable**	Required
Display test results	**display remote-ping results** [*admin-name operation-tag*]	Required You can execute the command in any view.

6 Configuring SNMP test on remote-ping client

Table 699 Configure SNMP test on remote-ping client

Operation	Command	Description
Enter system view	**system-view**	-
Enable the remote-ping client function	**remote-ping-agent enable**	Required By default, the remote-ping client function is disabled.
Create a remote-ping test group and enter its view	**remote-ping** *administrator-name operation-tag*	Required By default, no test group is configured.
Configure the test type	**test-type snmpquery**	Required By default, the test type is ICMP.

Table 699 Configure SNMP test on remote-ping client

Operation	Command	Description
Configure the destination IP address	**destination-ip** *ip-address*	Required By default, no destination address is configured.
Configure the source IP address	**source-ip** *ip-address*	Optional By default, no source IP address is configured.
Configure the source port	**source-port** port-number	Optional By default, no source port is configured.
Configure the number of probes per test	**count** *times*	Optional By default, each test makes one probe.
Configure the maximum number of history records that can be saved	**history-records** *number*	**Figure 237** Optional By default, the maximum number is 50.
Configure the automatic test interval	**frequency** *interval*	Optional By default, the automatic test interval is zero seconds, indicating no automatic test will be made.
Configure the probe timeout time	**timeout** *time*	Optional By default, a probe times out in three seconds.
Configure the type of service	**tos** *value*	Optional By default, the service type is zero.
Start the test	**test-enable**	Required
Display test results	**display remote-ping results** [*admin-name operation-tag*]	Required You can execute the command in any view.

7 Configuring TCP test on remote-ping client

Table 700 Configure TCP test on remote-ping client

Operation	Command	Description
Enter system view	**system-view**	-
Enable the remote-ping client function	**remote-ping-agent enable**	Required By default, the remote-ping client function is disabled.
Create a remote-ping test group and enter its view	remote-ping **administrator-name operation- tag**	Required By default, no test group is configured.

Table 700 Configure TCP test on remote-ping client

Operation	Command	Description
Configure the destination address	destination-ip ip-address	Required This IP address and the one configured on the remote-ping server for listening services must be the same. By default, no destination address is configured.
Configure the destination port	**destination-port** *port-number*	Required in a Tcpprivate test A Tcppublic test is a TCP connection test on port 7. Use the **remote-ping-server tcpconnect** *ip-address* 7 command on the server to configure the listening service port; otherwise the test will fail. No port number needs to be configured on the client; any destination port number configured on the client will not take effect. By default, no destination port number is configured.
Configure the source IP address	source-ip **ip-address**	Optional By default, the source IP address is not specified.
Configure the test type	**test-type** { **tcpprivate | tcppublic** }	Required By default, the test type is ICMP.
Configure the source port	source-port port-number	Optional By default, no source port is specified.
Configure the number of probes per test	count times	Optional By default, one probe is made per time.
Configure the automatic test interval	frequency interval	Optional By default, the automatic test interval is zero seconds, indicating no automatic test will be made.
Configure the probe timeout time	timeout time	Optional By default, a probe times out in three seconds.
Configure the maximum number of history records that can be saved	**history-records** *number*	**Figure 238** Optional By default, the maximum number is 50.
Configure the type of service	tos value	Optional By default, the service type is zero.
Start the test	**test-enable**	Required

Table 700 Configure TCP test on remote-ping client

Operation	Command	Description
Display test results	display remote-ping results [admin-name operation-tag]	Required The display command can be executed in any view.

8 Configuring UDP test on remote-ping client

Table 701 Configure UDP test on remote-ping client

Operation	Command	Description
Enter system view	system-view	-
Enable the remote-ping client function	remote-ping-agent enable	Required By default, the remote-ping client function is disabled.
Create a remote-ping test group and enter its view	remote-ping **administrator-name operation- tag**	Required By default, no test group is configured.
Configure the test type	test-type **{ udpprivate | udppublic** }	Required By default, the test type is ICMP.
Configure the destination address	destination-ip ip-address	Required This IP address and the one configured on the remote-ping server for listening service must be the same. By default, no destination address is configured.
Configure the destination port	destination-port **port-number**	■ Required in a Udpprivate test ■ A Udppublic test is a UDP connection test on port 7. Use the remote-ping-server udpecho ip-address 7 command on the server to configure the listening service port; otherwise the test will fail. No port number needs to be configured on the client; any destination port number configured on the client will not take effect. ■ By default, no destination port number is configured.
Configure the source IP address	source-ip **ip-address**	Optional By default, no source IP address is configured.
Configure the source port	source-port port-number	Optional By default, no source port is specified.

Table 701 Configure UDP test on remote-ping client

Operation	Command	Description
Configure the number of probes per test	count times	Optional By default, one probe is made per test.
Configure the maximum number of history records that can be saved	**history-records** *number*	**Figure 239** Optional By default, the maximum number is 50.
Configure the data packet size	datasize size	Optional By default, the data packet size is 100 bytes.
Configure the automatic test interval	frequency interval	Optional By default, the automatic test interval is zero seconds, indicating no automatic test will be made.
Configure the probe timeout time	timeout time	Optional By default, a probe times out in three seconds.
Configure the service type	tos value	Optional By default, the service type is zero.
Start the test	test-enable	Required
Display test results	display remote-ping results [admin-name operation-tag]	Required The display command can be executed in any view.

9 Configuring DNS test on remote-ping client

Table 702 Configure DNS test on remote-ping client

Operation	Command	Description
Enter system view	system-view	-
Enable the remote-ping client function	remote-ping-agent enable	Required By default, the remote-ping client function is disabled.
Create a remote-ping test group and enter its view	remote-ping **administrator-name operation- tag**	Required By default, no test group is configured.
Configure the source IP address	source-ip **ip-address**	Optional By default, no source IP address is specified.
Configure the test type	**test-type dns**	Required By default, the test type is ICMP.
Configure the number of probes per test	count times	Optional By default, one probe is made per test.

Table 702 Configure DNS test on remote-ping client

Operation	Command	Description
Configure the maximum number of history records that can be saved	**history-records** *number*	**Figure 240** Optional By default, the maximum number is 50.
Configure the automatic test interval	frequency interval	Optional By default, the automatic test interval is zero seconds, indicating no automatic test will be made.
Configure the probe timeout time	timeout time	Optional By default, a probe times out in three seconds.
Configure the type of service	tos value	Optional By default, the service type is zero.
Configure the domain name to be resolved	dns resolve-targetdomai domainname	Required By default, the domain name to be resolved by DNS is not specified.
Configure the IP address of the DNS server	dns-server ip-address	Required By default, no DNS server address is configured.
Start the test	test-enable	Required
Display test results	display remote-ping results [admin-name operation-tag]	Required The display command can be executed in any view.

Configuring Remote-ping client to send Trap messages

Trap messages are generated regardless of whether the remote-ping test succeeds or fails. You can specify whether to output Trap messages by enabling/disabling Trap sending.

Table 703 Configure the remote-ping client to send Trap messages

Operation	Command	Description
Enter system view	system-view	-
Enable the remote-ping client function	remote-ping-agent enable	Required By default, the remote-ping client function is disabled.
Create a remote-ping test group and enter its view	remote-ping **administrator-name operation- tag**	Required By default, no test group is configured.
Enable the remote-ping client to send Trap messages	send-trap { all | { probefailure | testcomplete | testfailure }***** }	Required By default, Trap sending is disabled.
Configure the number of consecutive unsuccessful remote-ping tests before Trap output	**test-failtimes times**	Optional By default, Trap messages are sent each time a test fails.

Table 703 Configure the remote-ping client to send Trap messages

Operation	Command	Description
Configure the number of consecutive unsuccessful remote-ping probes before Trap output	**probe-failtimes times**	Optional By default, Trap messages are sent each time a probe fails.

Displaying Remote-ping Configuration

After the above-mentioned configuration, you can use the **display** commands to view the results of the latest test and history information.

Table 704 Display remote-ping test results

Operation	Command	Description
Display test history	display remote-ping history [administrator-name operation-tag]	Available in any view.
Display the results of the latest test	display remote-ping results [administrator-name operation-tag]	

Remote-ping Configuration Example

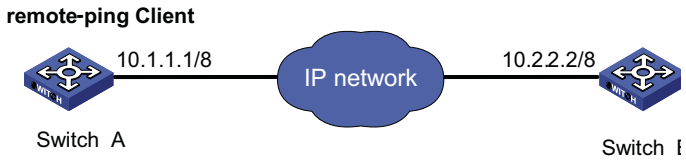
ICMP Test

Network requirements

The Switch 7750 serves as the remote-ping client. A remote-ping ICMP test between the switch and another switch uses ICMP to test the round trip time (RTT) for packets generated by the remote-ping client to travel to and back from the destination switch.

Network diagram

Figure 241 Network diagram for the ICMP test



Configuration procedure

- Configure remote-ping Client (Switch A):

  # Enable remote-ping client.

```
<7750> system-view
[7750] remote-ping-agent enable
```

  # Create a remote-ping test group, setting the administrator name to **administrator** and test tag to **ICMP**.

```
[7750] remote-ping administrator icmp
```

  # Configure the test type as **icmp**.

```
[7750-remote-ping-administrator-icmp] test-type icmp
```

Configure the destination IP address as 10.2.2.2.

```
[7750-remote-ping-administrator-icmp] destination-ip 10.2.2.2
```

Configure to make 10 probes per test.

```
[7750-remote-ping-administrator-icmp] count 10
```

Set the probe timeout time to 5 seconds.

```
[7750-remote-ping-administrator-icmp] timeout 5
```

Start the test.

```
[7750-remote-ping-administrator-icmp] test-enable
```

Set the maximum number of history records that can be saved to 5.

```
[7750-remote-ping-administrator-icmp] history-records 5
```

Display test results.

```
[7750-remote-ping-administrator-icmp] display remote-ping results administrator i
cmp
Remote-ping entry(admin administrator, tag icmp) test result:
      Destination ip address:10.2.2.2
      Send operation times: 10              Receive response times: 10
      Min/Max/Average Round Trip Time: 3/6/3
      Square-Sum of Round Trip Time: 145
      Last succeeded test time: 2000-4-2 20:55:12.3
  Extend result:
      SD Maximal delay: 0                   DS Maximal delay: 0
      Packet lost in test: 0%
      Disconnect operation number: 0        Operation timeout number: 0
      System busy operation number: 0       Connection fail number: 0
      Operation sequence errors: 0          Drop operation number: 0
      Other operation errors: 0
[7750-remote-ping-administrator-icmp] display remote-ping history administrator i
cmp
Remote-ping entry(admin administrator, tag icmp) history record:
    Index     Response    Status      LastRC      Time
        1            3         1           0    2000-04-02 20:55:12.3
        2            4         1           0    2000-04-02 20:55:12.3
        3            4         1           0    2000-04-02 20:55:12.2
        4            3         1           0    2000-04-02 20:55:12.2
        5            3         1           0    2000-04-02 20:55:12.2
```

For detailed output description, see the corresponding command manual.

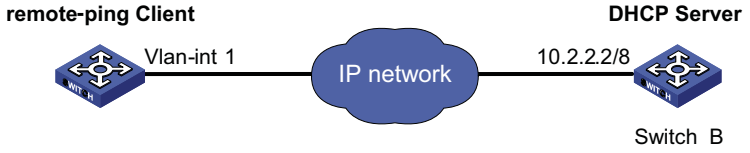
DHCP Test

Network requirements

Both the remote-ping client and the DHCP server are Switch 7750s. Perform a remote-ping DHCP test between the two switches to test the time required for the remote-ping client to obtain an IP address from the DHCP server.

Network diagram

Figure 242 Network diagram for the DHCP test



Configuration procedure

- Configure DHCP Server(Switch B):

  Configure DHCP server on Switch B. For specific configuration of DHCP server, refer to "DHCP Server Configuration" on page 593.

- Configure remote-ping Client (Switch A):

  # Enable the remote-ping client.

```
<7750> system-view
[7750] remote-ping-agent enable
```

  # Create a remote-ping test group, setting the administrator name to **administrator** and test tag to **DHCP**.

```
[7750] Remote-ping administrator dhcp
```

  # Configure the test type as **dhcp**.

```
[7750-remote-ping-administrator-dhcp] test-type dhcp
```

  # Configure the source interface, which must be a VLAN interface. Make sure the DHCP server resides on the network connected to this interface.

```
[7750-remote-ping-administrator-dhcp] source-interface Vlan-interface 1
```

  # Configure to make 10 probes per test.

```
[7750-remote-ping-administrator-dhcp] count 10
```

  # Set the probe timeout time to 5 seconds.

```
[7750-remote-ping-administrator-dhcp] timeout 5
```

  # Start the test.

```
[7750-remote-ping-administrator-dhcp] test-enable
```

  # Display test results

```
[7750-remote-ping-administrator-dhcp] display remote-ping results administra
tor dhcp
Remote-ping entry(admin administrator, tag dhcp) test result:
      Send operation times: 10              Receive response times: 10
      Min/Max/Average Round Trip Time: 1018/1037/1023
      Square-Sum of Round Trip Time: 10465630
      Last complete test time: 2000-4-3 9:51:30.9
  Extend result:
      SD Maximal delay: 0                   DS Maximal delay: 0
      Packet lost in test: 0%
      Disconnect operation number: 0        Operation timeout number: 0
      System busy operation number: 0       Connection fail number: 0
      Operation sequence errors: 0          Drop operation number: 0
      Other operation errors: 0
[7750-remote-ping-administrator-dhcp] display remote-ping history administra
tor dhcp
Remote-ping entry(admin administrator, tag dhcp) history record:
    Index     Response    Status      LastRC      Time
        1         1018         1           0    2000-04-03 09:51:30.9
        2         1037         1           0    2000-04-03 09:51:22.9
        3         1024         1           0    2000-04-03 09:51:18.9
        4         1027         1           0    2000-04-03 09:51:06.8
        5         1018         1           0    2000-04-03 09:51:00.8
        6         1020         1           0    2000-04-03 09:50:52.8
        7         1018         1           0    2000-04-03 09:50:48.8
        8         1020         1           0    2000-04-03 09:50:36.8
        9         1020         1           0    2000-04-03 09:50:30.8
       10         1028         1           0    2000-04-03 09:50:22.8
```

For detailed output description, see the corresponding command manual.

You can perform a remote-ping DHCP test only when no DHCP client is enabled on any interface. Otherwise, the DHCP Server sends the response to an interface enabled with the DHCP Client rather than to the source interface, thus resulting in remote-ping DHCP test failure.

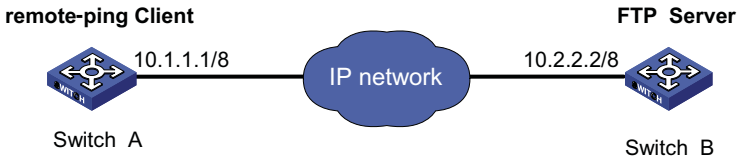
FTP Test

Network requirements

Both the remote-ping client and the FTP server are Switch 7750s. Perform a remote-ping FTP test between the two switches to test the connectivity to the specified FTP server and the time required to upload a file to the server after the connection is established. Both the username and password used to log in to the FTP server are **admin**. The file to be uploaded to the server is cmdtree.txt.

Network diagram

Figure 243 Network diagram for the FTP test



Configuration procedure

- Configure FTP Server (Switch B):

  Configure FTP server on Switch B. For specific configuration of FTP server, refer to"FTP and TFTP Configuration" on page 803.

- Configure remote-ping Client (Switch A):

  # Enable the remote-ping client.

```
<7750> system-view
[7750] remote-ping-agent enable
```

  # Create a remote-ping test group, setting the administrator name to **administrator** and test tag to **FTP**.

```
[7750] remote-ping administrator ftp
```

  # Configure the test type as **ftp**.

```
[7750-remote-ping-administrator-ftp] test-type ftp
```

  # Configure the IP address of the FTP server as 10.2.2.2.

```
[7750-remote-ping-administrator-ftp] destination-ip 10.2.2.2
```

  # Configure the FTP login username.

```
[7750-remote-ping-administrator-ftp] username admin
```

  # Configure the FTP login password.

```
[7750-remote-ping-administrator-ftp] password admin
```

  # Configure the type of FTP operation.

  [7750-remote-ping-administrator-ftp] ftp-operation put

  # Configure a file name for the FTP operation.

```
[7750-remote-ping-administrator-ftp] filename cmdtree.txt
```

Configure to make 10 probes per test.

```
[7750-remote-ping-administrator-ftp] count 10
```

Set the probe timeout time to 30 seconds.

```
[7750-remote-ping-administrator-ftp] timeout 30
```

Configure the source IP address

```
[7750-remote-ping-administrator-ftp] source-ip 10.1.1.1
```

Start the test.

```
[7750-remote-ping-administrator-ftp] test-enable
```

Display test results

```
[7750-remote-ping-administrator-ftp] display remote-ping results administrat
or ftp
Remote-ping entry(admin administrator, tag ftp) test result:
      Destination ip address:10.2.2.2
      Send operation times: 10              Receive response times: 10
      Min/Max/Average Round Trip Time: 3245/15891/12157
      Square-Sum of Round Trip Time: 1644458573
      Last complete test time: 2000-4-3 4:0:34.6
  Extend result:
      SD Maximal delay: 0                   DS Maximal delay: 0
      Packet lost in test: 0%
      Disconnect operation number: 0        Operation timeout number: 0
      System busy operation number: 0       Connection fail number: 0
      Operation sequence errors: 0          Drop operation number: 0
      Other operation errors: 0
[7750-remote-ping-administrator-ftp] display remote-ping history administrat
or ftp
Remote-ping entry(admin administrator, tag ftp) history record:
    Index     Response    Status      LastRC      Time
        1        15822         1           0    2000-04-03 04:00:34.6
        2        15772         1           0    2000-04-03 04:00:18.8
        3         9945         1           0    2000-04-03 04:00:02.9
        4        15891         1           0    2000-04-03 03:59:52.9
        5        15772         1           0    2000-04-03 03:59:37.0
        6        15653         1           0    2000-04-03 03:59:21.2
        7         9792         1           0    2000-04-03 03:59:05.5
        8         9794         1           0    2000-04-03 03:58:55.6
        9         9891         1           0    2000-04-03 03:58:45.8
       10         3245         1           0    2000-04-03 03:58:35.9
```

For detailed output description, see the corresponding command manual.



If you are downloading a file from the server, you do not need to specify an FTP operation type. For details, see "Configuring an FTP test on a remote-ping client".

HTTP Test

Network requirements

A 3Com Switch 7750 serves as the Remote-ping client, and a PC serves as the HTTP server. Perform a remote-ping HTTP test between the switch and the HTTP server to test the connectivity and the time required to download a file from the HTTP server after the connection to the server is established.

Network diagram

Figure 244 Network diagram for the HTTP test



Configuration procedure

- Configure the HTTP Server. Use a Windows 2003 Server as the HTTP server and follow the instructions in your Windows 2003 Server documentation.
- Configure remote-ping Client (Switch A):

  # Enable the remote-ping client.

```
<7750> system-view
[7750] remote-ping-agent enable
```

  # Create a remote-ping test group, setting the administrator name to **administrator** and test tag to **HTTP**.

```
[7750] Remote-ping administrator http
```

  # Configure the test type as **http**.

```
[7750-remote-ping-administrator-http] test-type http
```

  # Configure the IP address of the HTTP server as 10.2.2.2.

```
[7750-remote-ping-administrator-http] destination-ip 10.2.2.2
```

  # Configure to make 10 probes per test.

```
[7750-remote-ping-administrator-http] count 10
```

  # Set the probe timeout time to 30 seconds.

```
[7750-remote-ping-administrator-http] timeout 30
```

  # Start the test.

```
[7750-remote-ping-administrator-http] test-enable
```

  # Display test results

```
[7750-remote-ping-administrator-http] display remote-ping results administrator h
ttp
  Remote-ping entry(admin administrator, tag http) test result:
      Destination ip address:10.2.2.2
      Send operation times: 10              Receive response times: 10
      Min/Max/Average Round Trip Time: 47/87/74
      Square-Sum of Round Trip Time: 57044
      Last succeeded test time: 2000-4-2 20:41:50.4
  Extend result:
      SD Maximal delay: 0                   DS Maximal delay: 0
      Packet lost in test: 0%
      Disconnect operation number: 0        Operation timeout number: 0
      System busy operation number: 0       Connection fail number: 0
      Operation sequence errors: 0          Drop operation number: 0
      Other operation errors: 0
    Http result:
      DNS Resolve Time: 0                  HTTP Operation Time: 675
      DNS Resolve Min Time: 0              HTTP Test Total Time: 748
      DNS Resolve Max Time: 0              HTTP Transmission Successful Times: 10
      DNS Resolve Failed Times: 0          HTTP Transmission Failed Times: 0
```

```
      DNS Resolve Timeout Times: 0          HTTP Transmission Timeout Times: 0
      TCP Connect Time: 73                  HTTP Operation Min Time: 27
      TCP Connect Min Time: 5               HTTP Operation Max Time: 80
      TCP Connect Max Time: 20
      TCP Connect Timeout Times: 0
[7750-remote-ping-administrator-http] display remote-ping history administrator h
ttp
Remote-ping entry(admin administrator, tag http) history record:
    Index     Response    Status      LastRC      Time
        1           13         1           0    2000-04-02 15:15:52.5
        2            9         1           0    2000-04-02 15:15:52.5
        3            3         1           0    2000-04-02 15:15:52.5
        4            3         1           0    2000-04-02 15:15:52.5
        5            3         1           0    2000-04-02 15:15:52.5
        6            2         1           0    2000-04-02 15:15:52.4
        7            3         1           0    2000-04-02 15:15:52.4
        8            3         1           0    2000-04-02 15:15:52.4
        9            2         1           0    2000-04-02 15:15:52.4
       10            2         1           0    2000-04-02 15:15:52.4
```

For detailed output description, see the corresponding command manual.

For an HTTP test, if configuring the destination address as the host name, you must configure the IP address of the DNS server to resolve the host name into an IP address, which is the destination IP address of this HTTP test.

Jitter Test

Network requirements

Both the remote-ping client and the remote-ping server are Switch 7750s. Perform a remote-ping jitter test between the two switches to test the delay jitter of the UDP packets exchanged between this end (remote-ping client) and the specified destination end (remote-ping server).

Network diagram

Figure 245 Network diagram for the Jitter test



Configuration procedure

- Configure remote-ping Server (Switch B):

  # Enable the remote-ping server and configure the IP address and port to listen on.

```
<7750> system-view
[7750] remote-ping-server enable
[7750] remote-ping-server udpecho 10.2.2.2 9000
```

- Configure remote-ping Client (Switch A):

  # Enable the remote-ping client.

```
<7750> system-view
[7750] remote-ping-agent enable
```

  # Create a remote-ping test group, setting the administrator name to **administrator** and test tag to **Jitter**.

```
[7750] remote-ping administrator Jitter
```

Configure the test type as **jitter**

```
[7750-remote-ping-administrator-Jitter] test-type Jitter
```

Configure the IP address of the remote-ping server as 10.2.2.2.

```
[7750-remote-ping-administrator-Jitter] destination-ip 10.2.2.2
```

Configure the destination port on the remote-ping server.

```
[7750-remote-ping-administrator-Jitter] destination-port 9000
```

Configure to make 10 probes per test.

```
[7750-remote-ping-administrator-http] count 10
```

Set the probe timeout time to 30 seconds.

```
[7750-remote-ping-administrator-Jitter] timeout 30
```

Start the test.

```
[7750-remote-ping-administrator-Jitter] test-enable
```

Display test results

```
[7750-remote-ping-administrator-Jitter] display remote-ping results administrator
 Jitter
Remote-ping entry(admin administrator, tag Jitter) test result:
      Destination ip address:10.2.2.2
      Send operation times: 100             Receive response times: 100
      Min/Max/Average Round Trip Time: 9/21/13
      Square-Sum of Round Trip Time: 18623
      Last complete test time: 2000-4-2 8:14:58.2
  Extend result:
      SD Maximal delay: 10                  DS Maximal delay: 10
      Packet lost in test: 0%
      Disconnect operation number: 0        Operation timeout number: 0
      System busy operation number: 0       Connection fail number: 0
      Operation sequence errors: 0          Drop operation number: 0
      Other operation errors: 0
    Jitter result:
      RTT Number:100
      Min Positive SD:1                    Min Positive DS:1
      Max Positive SD:6                    Max Positive DS:8
      Positive SD Number:38                Positive DS Number:25
      Positive SD Sum:85                   Positive DS Sum:42
      Positive SD average:2                Positive DS average:1
      Positive SD Square Sum:267           Positive DS Square Sum:162
      Min Negative SD:1                    Min Negative DS:1
      Max Negative SD:6                    Max Negative DS:8
      Negative SD Number:30                Negative DS Number:24
      Negative SD Sum:64                   Negative DS Sum: 41
      Negative SD average:2                Negative DS average:1
      Negative SD Square Sum:200           Negative DS Square Sum:161
      SD lost packets number:0             DS lost packet number:0
      Unknown result lost packet number:0
[7750-remote-ping-administrator-Jitter] display remote-ping history administrator
 Jitter
Remote-ping entry(admin administrator, tag Jitter) history record:
    Index     Response    Status      LastRC      Time
        1          274         1           0    2000-04-02 08:14:58.2
        2          278         1           0    2000-04-02 08:14:57.9
        3          280         1           0    2000-04-02 08:14:57.6
        4          279         1           0    2000-04-02 08:14:57.3
        5          280         1           0    2000-04-02 08:14:57.1
        6          270         1           0    2000-04-02 08:14:56.8
        7          275         1           0    2000-04-02 08:14:56.5
        8          263         1           0    2000-04-02 08:14:56.2
        9          270         1           0    2000-04-02 08:14:56.0
       10          275         1           0    2000-04-02 08:14:55.7
```

For detailed output description, see the corresponding command manual.

SNMP Test

Network requirements

Both the remote-ping client and the SNMP Agent are Switch 7750s. Perform remote-ping SNMP tests between the two switches to test the time required from Switch A sends an SNMP query message to Switch B (SNMP Agent) to it receives a response from Switch B.

Network diagram

Figure 246 Network diagram for the SNMP test



Configuration procedure

- Configure SNMP Agent (Switch B):

  # Start SNMP agent and set SNMP version to V2C, read-only community name to **public**, and read-write community name to **private**.

```
<Sysname> system-view
[Sysname] snmp-agent
[Sysname] snmp-agent sys-info version v2c
[Sysname] snmp-agent community read public
[Sysname] snmp-agent community write private
```

- The SNMP network management function must be enabled on SNMP agent before it can receive response packets.
- The SNMPv2c version is used as reference in this example. This configuration may differ if the system uses any other version of SNMP. For details, see SNMP - RMON Operation Manual.
- Configure remote-ping Client (Switch A):

  # Enable the remote-ping client.

```
<7750> system-view
[7750] remote-ping-agent enable
```

  # Create a remote-ping test group, setting the administrator name to **administrator** and test tag to **snmp**.

```
[7750] Remote-ping administrator snmp
```

  # Configure the test type as **snmp**.

```
[7750-remote-ping-administrator-snmp] test-type snmpquery
```

  # Configure the destination IP address as 10.2.2.2.

```
[7750-remote-ping-administrator-snmp] destination-ip 10.2.2.2
```

  # Configure to make 10 probes per test.

```
[7750-remote-ping-administrator-snmp] count 10
```

  # Set the probe timeout time to 30 seconds.

```
[7750-remote-ping-administrator-snmp] timeout 30
```

Start the test.

```
[7750-remote-ping-administrator-snmp] test-enable
```

Display test results

```
[7750-remote-ping-administrator-snmp] display remote-ping results administrator s
nmp
Remote-ping entry(admin administrator, tag snmp) test result:
      Destination ip address:10.2.2.2
      Send operation times: 10              Receive response times: 10
      Min/Max/Average Round Trip Time: 9/11/10
      Square-Sum of Round Trip Time: 983
      Last complete test time: 2000-4-3 8:57:20.0
  Extend result:
      SD Maximal delay: 0                   DS Maximal delay: 0
      Packet lost in test: 0%
      Disconnect operation number: 0        Operation timeout number: 0
      System busy operation number: 0       Connection fail number: 0
      Operation sequence errors: 0          Drop operation number: 0
      Other operation errors: 0
[7750-remote-ping-administrator-snmp] display remote-ping history administrator s
nmp
Remote-ping entry(admin administrator, tag snmp) history record:
    Index     Response    Status      LastRC      Time
        1           10         1           0    2000-04-03 08:57:20.0
        2           10         1           0    2000-04-03 08:57:20.0
        3           10         1           0    2000-04-03 08:57:20.0
        4           10         1           0    2000-04-03 08:57:19.9
        5            9         1           0    2000-04-03 08:57:19.9
        6           11         1           0    2000-04-03 08:57:19.9
        7           10         1           0    2000-04-03 08:57:19.9
        8           10         1           0    2000-04-03 08:57:19.9
        9           10         1           0    2000-04-03 08:57:19.8
       10           10         1           0    2000-04-03 08:57:19.8
```

For detailed output description, see the corresponding command manual.

TCP Test (Tcpprivate Test) on the Specified Ports

Network requirements

Both the remote-ping client and the remote-ping server are Switch 7750s. Perform a remote-ping Tcpprivate test to test time required to establish a TCP connection between this end (Switch A) and the specified destination end (Switch B), with the port number set to 8000.

Network diagram

Figure 247 Network diagram for the Tcpprivate test



Configuration procedure

- Configure remote-ping Server (Switch B):

  # Enable the remote-ping server and configure the IP address and port to listen on.

```
<7750> system-view
[7750] remote-ping-server enable
[7750] remote-ping-server tcpconnect 10.2.2.2 8000
```

- Configure remote-ping Client (Switch A):

  # Enable the remote-ping client.

```
<7750> system-view
[7750] remote-ping-agent enable
```

  # Create a remote-ping test group, setting the administrator name to **administrator** and test tag to **tcpprivate**.

```
[7750] Remote-ping administrator tcpprivate
```

  # Configure the test type as **tcpprivate**.

```
[7750-remote-ping-administrator-tcpprivate] test-type tcpprivate
```

  # Configure the IP address of the remote-ping server as 10.2.2.2.

```
[7750-remote-ping-administrator-tcpprivate] destination-ip 10.2.2.2
```

  # Configure the destination port on the remote-ping server.

```
[7750-remote-ping-administrator-tcpprivate] destination-port 8000
```

  # Configure to make 10 probes per test.

```
[7750-remote-ping-administrator-tcpprivate] count 10
```

  # Set the probe timeout time to 5 seconds.

```
[7750-remote-ping-administrator-tcpprivate] timeout 5
```

  # Start the test.

```
[7750-remote-ping-administrator-tcpprivate] test-enable
```

  # Display test results.

```
[7750-remote-ping-administrator-tcpprivate] display remote-ping results administr
ator tcpprivate
Remote-ping entry(admin administrator, tag tcpprivate) test result:
      Destination ip address:10.2.2.2
      Send operation times: 10              Receive response times: 10
      Min/Max/Average Round Trip Time: 4/7/5
      Square-Sum of Round Trip Time: 282
      Last complete test time: 2000-4-2 8:26:2.9
  Extend result:
      SD Maximal delay: 0                   DS Maximal delay: 0
      Packet lost in test: 0%
      Disconnect operation number: 0        Operation timeout number: 0
      System busy operation number: 0       Connection fail number: 0
      Operation sequence errors: 0          Drop operation number: 0
      Other operation errors: 0
[7750-remote-ping-administrator-tcpprivate] display remote-ping history administr
ator tcpprivate
Remote-ping entry(admin administrator, tag tcpprivate) history record:
    Index     Response    Status      LastRC      Time
        1            4         1           0    2000-04-02 08:26:02.9
        2            5         1           0    2000-04-02 08:26:02.8
        3            4         1           0    2000-04-02 08:26:02.8
        4            5         1           0    2000-04-02 08:26:02.7
        5            4         1           0    2000-04-02 08:26:02.7
        6            5         1           0    2000-04-02 08:26:02.6
        7            6         1           0    2000-04-02 08:26:02.6
        8            7         1           0    2000-04-02 08:26:02.5
        9            5         1           0    2000-04-02 08:26:02.5
       10            7         1           0    2000-04-02 08:26:02.4
```

For detailed output description, see the corresponding command manual.

UDP Test (Udpprivate Test) on the Specified Ports

Network requirements

Both the remote-ping client and the remote-ping server are Switch 7750s. Perform a remote-ping Udpprivate test on the specified ports between the two switches to test the RTT of UDP packets between this end (remote-ping client) and the specified destination end (remote-ping server).

Network diagram

Figure 248 Network diagram for the Udpprivate test



Configuration procedure

- Configure remote-ping Server (Switch B):

  # Enable the remote-ping server and configure the IP address and port to listen on.

```
<7750> system-view
[7750] remote-ping-server enable
[7750] remote-ping-server udpecho 10.2.2.2 8000
```

- Configure remote-ping Client (Switch A):

  # Enable the remote-ping client.

```
<7750> system-view
[7750] remote-ping-agent enable
```

  # Create a remote-ping test group, setting the administrator name to administrator and test tag to **udpprivate**.

```
[7750] Remote-ping administrator udpprivate
```

  # Configure the test type as **udpprivate**.

```
[7750-remote-ping-administrator-udpprivate] test-type udpprivate
```

  # Configure the IP address of the remote-ping server as 10.2.2.2.

```
[7750-remote-ping-administrator-udpprivate] destination-ip 10.2.2.2
```

  # Configure the destination port on the remote-ping server.

```
[7750-remote-ping-administrator-udpprivate] destination-port 8000
```

  # Configure to make 10 probes per test.

```
[7750-remote-ping-administrator-udpprivate] count 10
```

  # Set the probe timeout time to 5 seconds.

```
[7750-remote-ping-administrator-udpprivate] timeout 5
```

  # Start the test.

```
[7750-remote-ping-administrator-udpprivate] test-enable
```

Display test results.

```
[7750-remote-ping-administrator-udpprivate] display remote-ping results administr
ator udpprivate
Remote-ping entry(admin administrator, tag udpprivate) test result:
      Destination ip address:10.2.2.2
      Send operation times: 10              Receive response times: 10
      Min/Max/Average Round Trip Time: 10/12/10
      Square-Sum of Round Trip Time: 1170
      Last complete test time: 2000-4-2 8:29:45.5
  Extend result:
      SD Maximal delay: 0                   DS Maximal delay: 0
      Packet lost in test: 0%
      Disconnect operation number: 0        Operation timeout number: 0
      System busy operation number: 0       Connection fail number: 0
      Operation sequence errors: 0          Drop operation number: 0
      Other operation errors: 0
[7750-remote-ping-administrator-udpprivate] display remote-ping history administr
ator udpprivate
Remote-ping entry(admin administrator, tag udpprivate) history record:
    Index     Response    Status      LastRC      Time
        1           11         1           0    2000-04-02 08:29:45.5
        2           12         1           0    2000-04-02 08:29:45.4
        3           11         1           0    2000-04-02 08:29:45.4
        4           11         1           0    2000-04-02 08:29:45.4
        5           11         1           0    2000-04-02 08:29:45.4
        6           11         1           0    2000-04-02 08:29:45.4
        7           10         1           0    2000-04-02 08:29:45.3
        8           10         1           0    2000-04-02 08:29:45.3
        9           10         1           0    2000-04-02 08:29:45.3
       10           11         1           0    2000-04-02 08:29:45.3
```

For detailed output description, see the corresponding command manual.

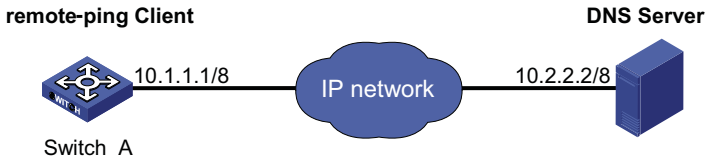
DNS Test

Network requirements

A Switch 7750 serves as the remote-ping client, and a PC serves as the DNS server. Perform a remote-ping DNS test between the switch and the DNS server to test the time required from the client sends a DNS request to it receives a resolution result from the DNS server.

Network diagram

Figure 249 Network diagram for the DNS test



Configuration procedure

- Use a Windows 2003 Server as the DNS server and follow the instructions in your Windows 2003 Server documentation to configure that server.
- Configure remote-ping Client (Switch A)

  # Enable the remote-ping client.

```
<7750> system-view
[7750] remote-ping-agent enable
```

Create a remote-ping test group, setting the administrator name to **administrator** and test tag to **dns**.

```
[7750] remote-ping administrator dns
```

Configure the test type as **dns**.

```
[7750-remote-ping-administrator-dns] test-type dns
```

Configure the IP address of the DNS server as 10.2.2.2.

```
[7750-remote-ping-administrator-dns] dns-server 10.2.2.2
```

Configure to resolve the domain name www.test.com.

```
[7750-remote-ping-administrator-dns] dns resolve-target www.test.com
```

Configure to make 10 probes per test.

```
[7750-remote-ping-administrator-dns] count 10
```

Set the probe timeout time to 5 seconds.

```
[7750-remote-ping-administrator-dns] timeout 5
```

Start the test.

```
[7750-remote-ping-administrator-dns] test-enable
```

Display test results.

```
[7750-remote-ping-administrator-dns] display remote-ping results administrator dn
s
Remote-ping entry(admin administrator, tag dns) test result:
      Destination ip address:10.2.2.2
      Send operation times: 10              Receive response times: 10
      Min/Max/Average Round Trip Time: 6/10/8
      Square-Sum of Round Trip Time: 756
      Last complete test time: 2006-11-28 11:50:40.9
  Extend result:
      SD Maximal delay: 0                   DS Maximal delay: 0
      Packet lost in test: 0%
      Disconnect operation number: 0        Operation timeout number: 0
      System busy operation number: 0       Connection fail number: 0
      Operation sequence errors: 0          Drop operation number: 0
      Other operation errors: 0
    Dns result:
      DNS Resolve Current Time: 10         DNS Resolve Min Time: 6
      DNS Resolve Times: 10                DNS Resolve Max Time: 10
      DNS Resolve Timeout Times: 0         DNS Resolve Failed Times: 0
[7750-remote-ping-administrator-dns] display remote-ping history administrator dn
s
Remote-ping entry(admin administrator, tag dns) history record:
    Index     Response    Status      LastRC      Time
        1           10         1           0    2006-11-28 11:50:40.9
        2           10         1           0    2006-11-28 11:50:40.9
        3           10         1           0    2006-11-28 11:50:40.9
        4            7         1           0    2006-11-28 11:50:40.9
        5            8         1           0    2006-11-28 11:50:40.9
        6            6         1           0    2006-11-28 11:50:40.9
        7            8         1           0    2006-11-28 11:50:40.9
        8            9         1           0    2006-11-28 11:50:40.9
        9            9         1           0    2006-11-28 11:50:40.9
       10            9         1           0    2006-11-28 11:50:40.9
```

For detailed output description, see the Switch 7750 Family Command Reference Guide.

82 RRPP CONFIGURATION

This board is supported if you have the special order modules listed in "RRPP on 3Com Switch 7750 Family" on page 908.

RRPP Overview

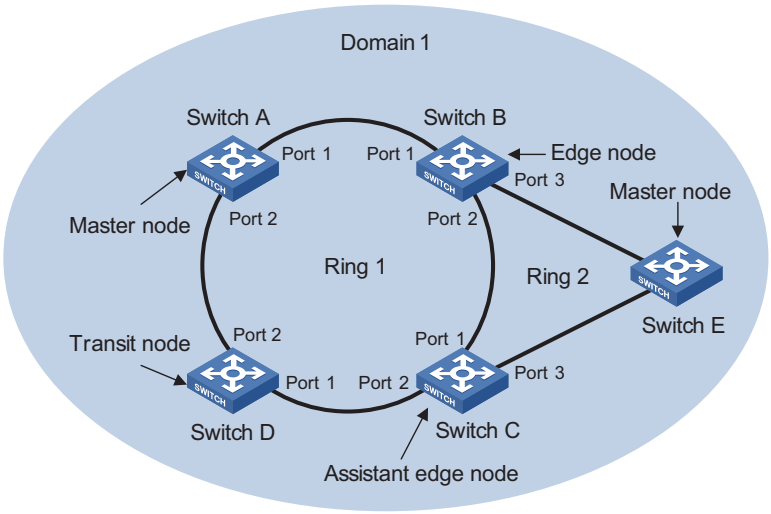
The rapid ring protection protocol (RRPP) is a link layer protocol designed for Ethernet rings. RRPP can prevent broadcast storm caused by data loops when the Ethernet rings are healthy, and restore rapidly the communication paths between nodes after a link is disconnected on the Ethernet ring network.

Compared with the Spanning Tree Protocol (STP), RRPP has the following characteristics:

- Dedicated to Ethernet ring topology
- Fast response

Basic Concepts of RRPP

Figure 250 RRPP networking



Domain

A domain consists of switches with the same domain ID and control VLAN. A domain can consist of multiple Ethernet rings, only one of which is the primary ring and the others are subrings. The ring roles are determined by user configuration. If there is only one Ethernet ring, you can configure the ring either as a primary ring or as a subring without making any difference in application.

As shown in Figure 250, Domain 1 is an RRPP domain, which consists of Ethernet ring 1 and ring 2. All the nodes on the Ethernet rings belong to the RRPP domain.

Ethernet ring

An Ethernet ring is a ring-shaped Ethernet topology, on which a RRPP domain is based. An RRPP domain consists of a primary ring and one or more subrings. In configuration, the level of the primary ring is level 0, and that of the subrings is level 1.

As shown in Figure 250, RRPP domain 1 consists of ring 1 and ring 2. If their levels are set to level 0 and level 1 respectively, ring 1 is the primary ring and ring 2 is the subring.

Each ring is in one of the following two states:

- Healthy state: The physical links of the ring network are connected.
- Broken state: A certain physical link is disconnected on the ring network.

Control VLAN and data VLAN

- A control VLAN is a special VLAN used to transfer RRPP packets. The port on each switch for connecting the switch with the Ethernet ring belongs to the control VLAN, and only the ports connected to the Ethernet ring can be added to the control VLAN. It is not allowed to configure an IP address for the interface of the control VLAN. You can configure the control VLAN of the primary ring. The control VLAN of the subring is assigned by the system automatically. The ID of the subring control VLAN is the ID of the primary ring control VLAN plus 1.
- A data VLAN is used to transfer data packets. A data VLAN contains the ports connecting the switch with the Ethernet ring network and other ports.

Node

Every switch on an Ethernet ring network is a node. Node roles are as follows:

- Master node: The node that initiates loop detection and prevents data loops prevention is the master node. Each ring has one and only one master node.
- Transit node: All nodes other than the master node on a ring are transit nodes.
- Edge node: An edge node is located on the primary ring and a subring at the same time. An edge node serves as a transit node on the primary ring and an edge node on a subring. In an RRPP domain, there are two edge nodes on a subring. You must specify any one of them as assistant edge node so far the configuration can tell the difference between the edge node and assistant edge node.

The node roles are determined by user configuration. As shown in Figure 250, Switch A is the master node on ring 1, and Switch B, Switch C and Switch D are transit nodes on ring 1. Switch B and Switch C are edge nodes because they are both on ring 2. You can specify one of them as edge node, and the other as assistant edge node.

Primary port and secondary port

The master node and each of the transit nodes are connected to an Ethernet ring through two ports, of which one is the primary port and the other is the secondary port. The node roles are determined by user configuration.

- The primary port and secondary port of the master node

The primary port of the master node transmits the loop detection packet, and the secondary port of the master node receives the loop detection packet.

When an Ethernet ring is in the healthy state, the secondary port of the master node allows only RRPP packets to pass, but logically blocks data packets in data VLANs.

When the Ethernet ring is in the broken state, the secondary port of the master node stops blocking the data VLAN and begins to forwards data packets in data VLANs.

- The primary and secondary ports of a transit node are functionally the same.

The node roles are determined by user configuration. As shown in Figure 250, Switch A is the master node of Ring 1. Port 1 and Port 2 of Switch A are the primary port and secondary port respectively. Switch B, Switch C and Switch D are the transit nodes on ring 1, and their respective port 1 and port 2 are the primary port and secondary port on ring 1.

Subring protocol messages are processed as data packets in the primary ring. Thus, when the secondary port on the master node of the primary ring, or the RRPP ports (including the primary and secondary ports) on the transit node are blocked, both data packets and subring protocol messages cannot pass through the port. After the ports are unblocked, these packets or messages can pass through the ports.

Common port and edge port

Of the two ports connecting an edge node (or assistant edge node) to a subring, one is the common port and the other is the edge port of the node. The common port connects the edge node to the primary ring and a subring at the same time. An edge port is connected only with a subring.

Conceptually, a common port is not treated as a port on the subring. Instead, it is a part of the primary ring. In another word, the common link is a link on the primary ring instead of the subring. Status change of a public link is only reported to the master node of the primary ring and the master node of the subring needs not know about the change.

The node roles are determined by user configuration. As shown in Figure 250, Switch B and Switch C are on ring 1 and ring 2 at the same time. Port 2 of Switch B and Port 1 of Switch C connect the primary and a subring, so they are common ports. Port 3 of Switch B and Port 3 of Switch C connect only the subring, so they are edge ports.

MAC address FDB

The Layer 2 forwarding database (FDB) on a switch is updated through the source MAC address auto-learning function of the switch.

Timer

Two timers, Hello timer and Fail timer, are involved when the master node sends and receives RRPP packets.

- Hello timer: Defines the time interval at which the primary port of the master node sends the health detection packet.

- Fail timer: Defines the timeout time for the secondary port of the master node to receive health detection packets. The value of Fail timer must be greater than or equal to three times the Hello timer value.

RRPP Message Type

The following table describes RRPP message types.

Table 705 RRPP messages

Message	Description
HEALTH (HELLO)t	The master node sends the HELLO message to detect whether the ring network is complete.
LINK DOWN	A transit node sends this message to notify the master node that a port is DOWN and the physical ring is disconnected.
COMMON- FLUSH-FDB	The master node sends this message to tell all the transit nodes to refresh their respective MAC address FDB.
COMPLETE- FLUSH-FDB	The master node sends this message to tell all the transit nodes to refresh their respective MAC address FDB and unblock the ports in the blocked data VLANs.
EDGE-HELLO	This message is generated by the edge node of a subring and received by the assistant edge node in the same subring. The subring uses this message to check the integrity of the primary ring in the home domain.
MAJOR-FAULT	This message is generated by the assistant edge node of a subring. If the assistant edge node does not receive the EDGE-HELLO from the edge node within the specified period, it reports to the edge node that a fault exists in the primary ring of the home domain.

Basic Principles of RRPP

Link DOWN notification mechanism

When detecting a port in the RRPP domain is down, a transit node sends the LINK DOWN packet immediately to the master node. After receiving the LINK DOWN packet, the master node unblocks the data VLAN of the secondary port, and sends the Common Flush packet to tell all transit nodes to refresh their respective MAC address FDB and ARP table.

Polling mechanism

The primary port of the master node periodically sends the health detection packet in a control VLAN.

- If the secondary port of the master node receives the health detection packet, this indicates that the ring link is complete, and the master node will keep the secondary port blocked.
- If the secondary port of the master node fails to receive the health detection packet within the predefined timeout time, this indicates that a failure has occurred to the ring link. In this case, the master node unblocks the data VLANs on the secondary port, and sends the Common Flush packet to tell all transit nodes to refresh their respective MAC address FDB and ARP table.

Ring recovery

The master node may detect that the ring has recovered a period time after the RRPP domain port on a transit node becomes UP again. In this period, a temporary data loop may occur in data VLANs, which can cause broadcast storm.

To avoid temporary data loops, when detecting the port through which it connects to the ring network becomes UP again, a transit node blocks the port temporarily (only control VLAN packets are permitted to pass), and keeps the port blocked until it receives the Complete Flush packet from the master node.

The following details how to unblock the temporarily blocked port:

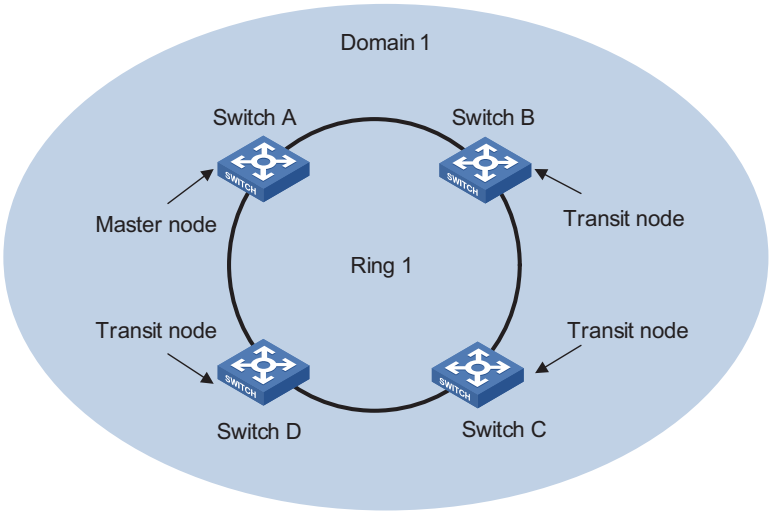
- When the master node is in the Fail status, if the secondary port receives the HEALTH sent by the primary port, the master node believes that the ring network has been recovered. Thus, the node status is transited to the Complete status and the master node sends the Complete Flush message through the primary port to request the transit node to update the FDB and unblock the temporarily blocked port. After the transit node receives the Complete Flush message, it unblocks the temporarily blocked port.
- If the transit node does not receive the Complete Flush message after the Fail timer expires, it automatically unblocks the temporarily blocked port.

Typical Networking of RRPP

To ensure normal RRPP operation, you must configure RRPP correctly. Here are several typical networking applications.

Single ring network

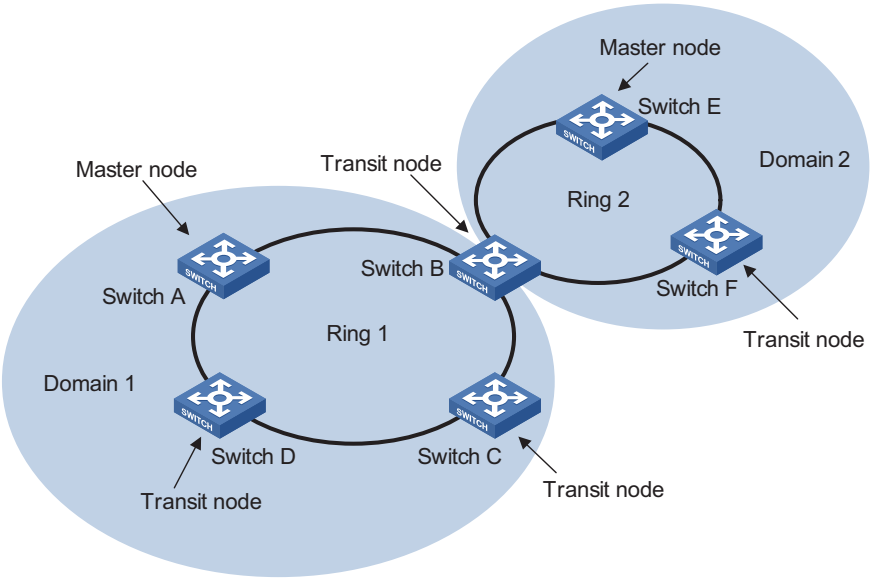
Figure 251 Single ring network



There is only one ring in the network topology. In this case, only one RRPP domain is to be defined.

Tangent ring networking

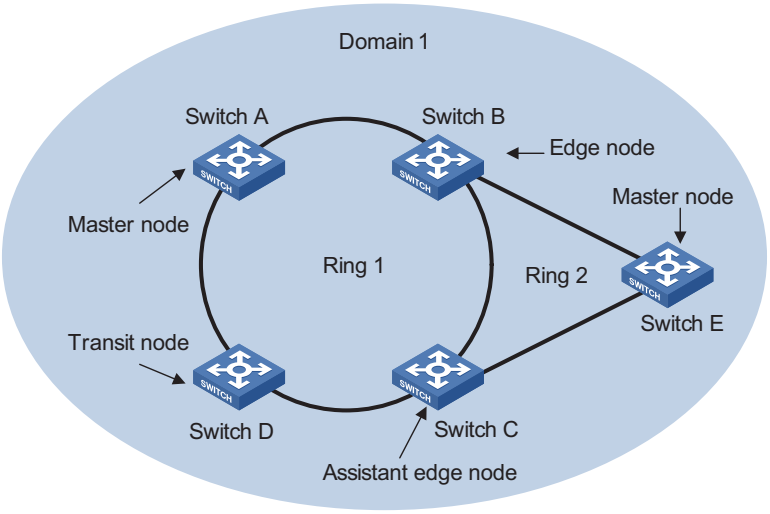
Figure 252 Tangent ring networking



There are two or more rings in the network topology and only one common node exists between each pair of rings. In this case, one RRPP domain must be defined for each ring.

Intersectant ring networking

Figure 253 Intersectant ring networking



There are two or more rings in the network topology and two common nodes exist between each pair of rings. In this case, only one RRPP domain is to be defined, in which one ring must be defined as the primary ring and the rest as subrings.

RRPP on 3Com Switch 7750 Family

To employ RRPP on a Switch 7750 Ethernet switch, make sure that:

- The chassis comes with the silk print **XGbus**.

- For 3Com Switches 7754, 7757, and 7758, BootROM version 527 must be used.
- The CPLD version of the I/O Modules is not lower than 005.

Ports that support RRPP are:

- The four Gigabit SFP ports on the 96Gbps Switch Fabric.
- Gigabit SFP ports/10 Gigabit ports on LS81T12PE, LS81P12TE, LS81GP8UB, LS81TGX2, LS81TGX4, LS81T32P, LS81T16P, and LS81GP48 I/O Modules.



- *For information about the chassis, Fabric, and I/O Module of 3Com Switches 7754, 7757, and 7758 , refer to 3Com Switch 7750 Family Installation Guide.*

As for the above-mentioned ports, to make RRPP-related configuration to take effect, you need also to make sure that:

- The ports are Trunk ports and permit packets of data VLANs.
- The ports cannot be aggregation ports.
- MSTP, QinQ, 802.1x or Voice VLAN is not enabled on the ports.

Master Node Configuration

Configuration Prerequisites

The switch ports connecting the Ethernet rings have been configured as trunk ports. All ports allow data VLAN packets to pass. And STP has been disenabled on all the ports connecting the Ethernet rings.

Master Node Configuration Tasks

The following table describes the master node configuration tasks.

Table 706 Configure the master node

Operation	Command	Description
Enter system view	**system-view**	-
Create an RRPP domain, and enter RRPP domain view	**rrpp domain** *domain-id*	Required. The command prompt of RRPP domain view depends on the *domain-id* you input.
Specify a control VLAN for the RRPP domain	**control-vlan** *vlan-id*	Required
Specify the current switch as the primary node of a ring, and specify the primary port and the secondary port of the node	**ring** *ring-id* **node-mode master** [**primary-port** *pri-port*]] **secondary-port** *sec-port*] **level** *level-value*	Required. Level 0 identifies the primary ring and level 1 identifies a subring.
Configure RRPP domain timers	**timer hello-timer** *hello-value* **fail-timer** *fail-value*	Optional. By default, the Hello timer is set to 1 second, and the Fail timer to 3 seconds.
Enable an RRPP ring	**ring** *ring-id* **enable**	Required

Table 706 Configure the master node

Operation	Command	Description
Return to system view	**quit**	-
Enable the RRPP protocol	**rrpp enable**	Required
Display the brief information of all RRPP domains configured on the switch	**display rrpp brief**	Optional. You can execute the **display** command in any view
Display RRPP configuration details on the switch	**display rrpp verbose domain** *domain-id* [**ring** *ring-id*]	
Display RRPP packet statistics of the switch	**display rrpp statistics domain** *domain-id* [**ring** *ring-id*]	
Clear the RRPP statistics information	**reset rrpp statistics domain** *domain-id* [**ring** *ring-id*]	Optional You can execute the **reset** command in user view.

CAUTION:

- *The control VLAN of an RRPP domain cannot be a static VLAN already created on the switch. If you configure a dynamic VLAN as the control VLAN of an RRPP domain, the VLAN becomes a static VLAN automatically.*
- *You are not recommended to configure a VLAN as both an RRPP control VLAN and a remote-probe VLAN. (Refer to "Mirroring Configuration" on page 685 for information about remote-probe VLAN.)*
- *You are not recommended to configure a VLAN as both an RRPP control VLAN and an isolate-user-VLAN/sub VLAN. (Refer to "Isolate-User-VLAN Configuration" on page 113 and "Configuring a Sub VLAN" on page 122.)*
- *Before creating an RRPP ring, you must create a control VLAN.*
- *RRPP and loopback test functions are mutually exclusive. You must disenable the loopback test on the primary/secondary port of the master/transit node and the common/edge port of the edge node.*
- *When deleting an RRPP domain by using the **undo rrpp domain** command, make sure no RRPP ring exists in the RRPP domain.*
- *The ring ID must be unique in the same RRPP domain.*

Master Node Configuration Example

Network requirements

- Define the switch as a node in RRPP domain 1
- Define VLAN 4092 as the control VLAN
- Define the switch as the master node on primary ring 1 in RRPP domain 1, GigabitEthernet2/0/1 as the primary port, and GigabitEthernet2/0/2 as the secondary port.
- Set the Hello timer and Fail time to 2 seconds and 7 seconds respectively.

Configuration procedure

CAUTION: *Make sure that the switch ports connecting the Ethernet rings have been configured as trunk ports. All ports allow data VLAN packets to pass. And STP has been disenabled on all the ports connecting the Ethernet rings.*

```
<SW7750> system-view
[SW7750] rrpp domain 1
[SW7750-rrpp-domain-1] control-vlan 4092
[SW7750-rrpp-domain-1] ring 1 node-mode master primary-port GigabitE
thernet2/0/1 secondary-port GigabitEthernet2/0/2 level 0
[SW7750-rrpp-domain-1] timer hello-timer 2 fail-timer 7
[SW7750-rrpp-domain-1] ring 1 enable
[SW7750-rrpp-domain-1] quit
[SW7750] rrpp enable
[SW7750] display rrpp brief
[SW7750] display rrpp verbose domain 1
[SW7750] display rrpp statistics domain 1
```

Transit Node Configuration

Configuration Prerequisites

The switch ports connecting the Ethernet rings have been configured as trunk ports. All ports allow data VLAN packets to pass. And STP has been disenabled on all the ports connecting the Ethernet rings.

Transit Node Configuration Tasks

The following table describes the transit node configuration tasks.

Table 707 Configure a transit node

Operation	Command	Description
Enter system view	**system-view**	-
Create an RRPP domain, and enter RRPP domain view	**rrpp domain** *domain-id*	Required. The command prompt of RRPP domain view depends on the *domain-id* you input.
Specify a control VLAN for the RRPP domain	**control-vlan** *vlan-id*	Required
Specify the current switch as the transit node of a ring, and specify the primary port and the secondary port of the node	**ring** *ring-id* **node-mode transit** [**primary-port** *pri-port*] [**secondary-port** *sec-port*] **level** *level-value*	Required. Level 0 identifies the primary ring and level 1 identifies a subring.
Enable an RRPP ring	**ring** *ring-id* **enable**	Required
Return to system view	**quit**	-
Enable RRPP	**rrpp enable**	Required
Display the brief information of all RRPP domains configured on the switch	**display rrpp brief**	Optional. You can execute the **display** command in any view
Display RRPP configuration details on the switch	**display rrpp verbose domain** *domain-id* [**ring** *ring-id*]	
Display the RRPP packet statistics on the switch	**display rrpp statistics domain** *domain-id* [**ring** *ring-id*]	
Clear the RRPP statistics information	**reset rrpp statistics domain** *domain-id* [**ring** *ring-id*]	Optional You can execute the **reset** command in user view.

CAUTION:

- *The control VLAN of an RRPP domain cannot be a static VLAN already created on the switch. If you configure a dynamic VLAN as the control VLAN of an RRPP domain, the VLAN becomes a static VLAN automatically.*
- *You are not recommended to configure a VLAN as both an RRPP control VLAN and a remote-probe VLAN. (Refer to "Mirroring Configuration" on page 685 for information about remote-probe VLAN.)*
- *You are not recommended to configure a VLAN as both an RRPP control VLAN and an isolate-user-VLAN/sub VLAN. (Refer to "Isolate-User-VLAN Configuration" on page 113 and "Configuring a Sub VLAN" on page 122.)*
- *Before creating an RRPP ring, you must create a control VLAN.*
- *RRPP and loopback test functions are mutually exclusive. You must disenable the loopback test on the primary/secondary port of the master/transit node and the common/edge port of the edge node.*
- *When deleting an RRPP domain by using the undo rrpp domain command, make sure no RRPP ring exists in the RRPP domain.*
- *The ring ID must be unique in the same RRPP domain.*

Transit Node Configuration Example

Network requirements

- Define the switch as a node in RRPP domain 1.
- Define VLAN 4092 as the control VLAN
- Define the switch as a transit node on primary ring 1 in RRPP domain 1, GigabitEthernet2/0/1 as the primary port, and GigabitEthernet2/0/2 as the secondary port.

Configuration procedure

CAUTION: *Make sure that the switch ports connecting the Ethernet rings have been configured as trunk ports. All ports allow data VLAN packets to pass. And STP has been disenabled on all the ports connecting the Ethernet rings.*

```
<SW7750> system-view
[SW7750] rrpp domain 1
[SW7750-rrpp-domain-1] control-vlan 4092
[SW7750-rrpp-domain-1] ring 1 node-mode transit primary-port Gigabit
Ethernet2/0/1 secondary-port GigabitEthernet2/0/2 level 0
[SW7750-rrpp-domain-1] ring 1 enable
[SW7750-rrpp-domain-1] quit
[SW7750] rrpp enable
[SW7750] display rrpp brief
[SW7750] display rrpp verbose domain 1
[SW7750] display rrpp statistics domain 1
```

Edge Node Configuration

Configuration Prerequisites

The switch ports connecting the Ethernet rings have been configured as trunk ports. All ports allow data VLAN packets to pass. And STP has been disenabled on all the ports connecting the Ethernet rings.

Edge Node Configuration Tasks

The following table describes the edge node configuration tasks.

Table 708 Configure an edge node

Operation	Command	Description
Enter system view	**system-view**	-
Create an RRPP domain, and enter RRPP domain view	**rrpp domain** *domain-id*	Required. The command prompt of RRPP domain view depends on the *domain-id* you input.
Specify a control VLAN for the RRPP domain	**control-vlan** *vlan-id*	Required
Specify the current switch as a transit node of the primary ring, and specify the primary port and the secondary port	**ring** *ring-id* **node-mode transit** [**primary-port** *pri-port*] [**secondary-port** *sec-port*] **level** *level-value*	Required. Level 0 identifies the primary ring and level 1 identifies a subring.
Specify the current switch as an edge node of the subring, and specify a common port and an edge port	**ring** *ring-id* **node-mode edge** [**common-port** *comm-port*] [**edge-port** *edge-port*]	Required
Enable the primary ring	**ring** *ring-id* **enable**	Required
Enable the subring	**ring** *ring-id* **enable**	Required
Return to system view	**quit**	-
Enable RRPP	**rrpp enable**	Required
Display the brief information of all RRPP domains configured on the switch	**display rrpp brief**	Optional. You can execute the **display** command in any view
Display RRPP configuration details on the switch	**display rrpp verbose domain** *domain-id* [**ring** *ring-id*]	
Display the RRPP packet statistics on the switch	**display rrpp statistics domain** *domain-id* [**ring** *ring-id*]	
Clear the RRPP statistics information	**reset rrpp statistics domain** *domain-id* [**ring** *ring-id*]	Optional You can execute the **reset** command in user view.

To clear the RRPP statistics information, use the **reset rrpp statistics domain** *domain-id* [**ring** *ring-id*] command.



CAUTION:

- *The control VLAN of an RRPP domain cannot be a static VLAN already created on the switch. If you configure a dynamic VLAN as the control VLAN of an RRPP domain, the VLAN becomes a static VLAN automatically.*
- *You are not recommended to configure a VLAN as both an RRPP control VLAN and a remote-probe VLAN. (Refer to "Mirroring Configuration" on page 685 for information about remote-probe VLAN.)*
- *You are not recommended to configure a VLAN as both an RRPP control VLAN and an isolate-user-VLAN/sub VLAN. (Refer to "Isolate-User-VLAN Configuration" on page 113 and "Configuring a Sub VLAN" on page 122.)*

- *Before creating an RRPP ring, you must create a control VLAN.*
- *RRPP and loopback test functions are mutually exclusive. You must disenable the loopback test on the primary/secondary port of the master/transit node and the common/edge port of the edge node.*
- *When deleting an RRPP domain by using the undo rrpp domain command, make sure no RRPP ring exists in the RRPP domain.*
- *The ring ID must be unique in the same RRPP domain.*

Edge Node Configuration Example

Network requirements

- Define the switch as a node in RRPP domain 1.
- Define VLAN 4092 as the control VLAN
- Define the switch as a transit node on primary ring 1 in RRPP domain 1, GigabitEthernet2/0/1 as the primary port, and GigabitEthernet2/0/2 as the secondary port.
- Define the switch as an edge node on subring 2 in RRPP domain 1, the port GigabitEthernet2/0/2 as the common port, the port GigabitEthernet2/0/4 as the edge port.

Configuration procedure



CAUTION: *Make sure that the switch ports connecting the Ethernet rings have been configured as trunk ports. All ports allow data VLAN packets to pass. And STP has been disenabled on all the ports connecting the Ethernet rings.*

```
<SW7750> system-view
[SW7750] rrpp domain 1
[SW7750-rrpp-domain-1] control-vlan 4092
[SW7750-rrpp-domain-1] ring 1 node-mode transit primary-port Gigabit
Ethernet2/0/1 secondary-port GigabitEthernet2/0/2 level 0
[SW7750-rrpp-domain-1] ring 2 node-mode edge common-port GigabitEthe
rnet 2/0/2 edge-port GigabitEthernet 2/0/4
[SW7750-rrpp-domain-1] ring 1 enable
[SW7750-rrpp-domain-1] ring 2 enable
[SW7750-rrpp-domain-1] quit
[SW7750] rrpp enable
[SW7750] display rrpp brief
[SW7750] display rrpp verbose domain 1
[SW7750] display rrpp statistics domain 1
```

Assistant Edge Node Configuration

Configuration Prerequisites

The switch ports connecting the Ethernet rings have been configured as trunk ports. All ports allow data VLAN packets to pass. And STP has been disenabled on all the ports connecting the Ethernet rings.

Assistant Edge Node Configuration Tasks

The following table describes the assistant edge node configuration tasks.

Table 709 Configure an assistant edge node

Operation	Command	Description
Enter system view	**system-view**	-
Create an RRPP domain, and enter RRPP domain view	**rrpp domain** *domain-id*	Required. The command prompt of RRPP domain view depends on the *domain-id* you input.
Specify a control VLAN for the RRPP domain	**control-vlan** *vlan-id*	Required
Specify the current switch as a transit node of the primary ring, and specify the primary port and the secondary port	**ring** *ring-id* **node-mode transit** [**primary-port** *pri-port*] [**secondary-port** *sec-port*] **level** *level-value*	Required. Level 0 identifies the primary ring and level 1 identifies a subring.
Specify the current switch as an assistant edge node of the subring, and specify a common port and an edge port	**ring** *ring-id* **node-mode assistant-edge** [**common-port** *comm-port*] [**edge-port** *edge-port*]	Required
Enable the primary ring	**ring** *ring-id* **enable**	Required
Enable the subring	**ring** *ring-id* **enable**	Required
Return to system view	**quit**	-
Enable RRPP	**rrpp enable**	Required
Display the brief information of all RRPP domains configured on the switch	**display rrpp brief**	Optional. You can execute the **display** command in any view
Display RRPP configuration details on the switch	**display rrpp verbose domain** *domain-id* [**ring** *ring-id*]	
Display the RRPP packet statistics on the switch	**display rrpp statistics domain** *domain-id* [**ring** *ring-id*]	
Clear the RRPP statistics information	**reset rrpp statistics domain** *domain-id* [**ring** *ring-id*]	Optional You can execute the **reset** command in user view.

To clear the RRPP statistics information, use the **reset rrpp statistics domain** *domain-id* [**ring** *ring-id*] command.

CAUTION:

- *The control VLAN of an RRPP domain cannot be a static VLAN already created on the switch. If you configure a dynamic VLAN as the control VLAN of an RRPP domain, the VLAN becomes a static VLAN automatically.*
- *You are not recommended to configure a VLAN as both an RRPP control VLAN and a remote-probe VLAN. (Refer to "Mirroring Configuration" on page 685 for information about remote-probe VLAN.)*
- *You are not recommended to configure a VLAN as both an RRPP control VLAN and an isolate-user-VLAN/sub VLAN. (Refer to "Isolate-User-VLAN Configuration" on page 113 and "Configuring a Sub VLAN" on page 122.)*

- *Before creating an RRPP ring, you must create a control VLAN.*
- *RRPP and loopback test functions are mutually exclusive. You must disenable the loopback test on the primary/secondary port of the master/transit node and the common/edge port of the edge node.*
- *When deleting an RRPP domain by using the undo rrpp domain command, make sure no RRPP ring exists in the RRPP domain.*
- *The ring ID must be unique in the same RRPP domain.*

Assistant Edge Node Configuration Example

Network requirements

- Define the switch as a node in RRPP domain 1.
- Define VLAN 4092 as the control VLAN
- Define the switch as a transit node in primary ring 1 in RRPP domain 1, the port GigabitEthernet2/0/1 as the primary port, the port GigabitEthernet2/0/2 as the secondary port.
- Define the switch as an assistant edge node on subring 2 in the RRPP domain 1, the port GigabitEthernet2/0/2 as the common port, and the port GigabitEthernet2/0/4 as the edge port.

Configuration procedure



CAUTION: *Make sure that the switch ports connecting the Ethernet rings have been configured as trunk ports. All ports allow data VLAN packets to pass. And STP has been disenabled on all the ports connecting the Ethernet rings.*

```
<SW7750> system-view
[SW7750] rrpp domain 1
[SW7750-rrpp-domain-1] control-vlan 4092
[SW7750-rrpp-domain-1] ring 1 node-mode transit primary-port Gigabit
Ethernet2/0/1 secondary-port GigabitEthernet2/0/2 level 0
[SW7750-rrpp-domain-1] ring 2 node-mode assistant-edge common-port G
igabitEthernet 2/0/2 edge-port GigabitEthernet 2/0/4
[SW7750-rrpp-domain-1] ring 1 enable
[SW7750-rrpp-domain-1] ring 2 enable
[SW7750-rrpp-domain-1] quit
[SW7750] rrpp enable
[SW7750] display rrpp brief
[SW7750] display rrpp verbose domain 1
[SW7750] display rrpp statistics domain 1
```

Configuration Example

Single Ring Network Configuration Example

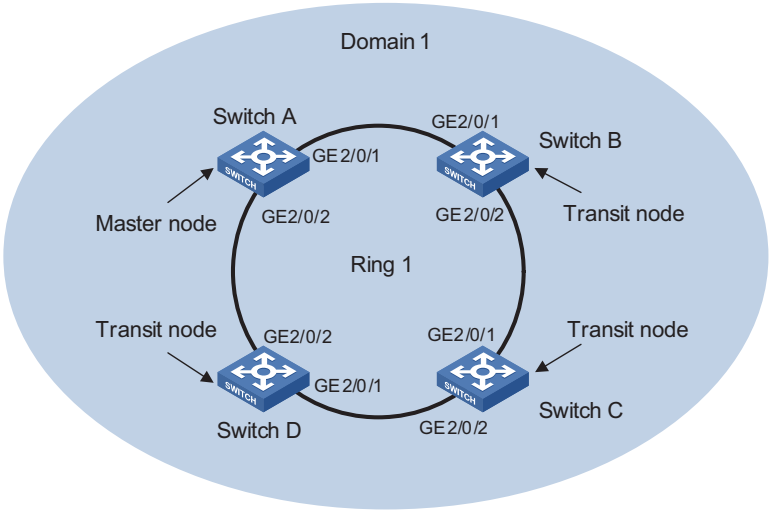
Network requirements

- Switch A, Switch B, Switch C and Switch D constitute RRPP domain 1
- VLAN 4092 is the control VLAN of RRPP domain 1
- Switch A, Switch B, Switch C and Switch D constitute primary ring 1
- Switch A serves as the master node of the primary ring, its GigabitEthernet2/0/1 is the primary port, and GigabitEthernet2/0/2 is the secondary port

- Switch B, Switch C and Switch D are transit nodes of the primary ring. Their respective GigabitEthernet2/0/1 and GigabitEthernet2/0/2 serve as the primary and secondary ports
- The default values are used for the timers on the primary ring

Network diagram

Figure 254 Network diagram for single ring topology



Configuration procedure

⚠ ***CAUTION:*** *Make sure that the switch ports connecting the Ethernet rings have been configured as trunk ports. All ports allow data VLAN packets to pass. And STP has been disenabled on all the ports connecting the Ethernet rings.*

- Configure Switch A

```
<SW7750> system-view
[SW7750] rrpp domain 1
[SW7750-rrpp-domain-1] control-vlan 4092
[SW7750-rrpp-domain-1] ring 1 node-mode master primary-port GigabitE
thernet2/0/1 secondary-port GigabitEthernet2/0/2 level 0
[SW7750-rrpp-domain-1] ring 1 enable
[SW7750-rrpp-domain-1] quit
[SW7750] rrpp enable
```

- Configure Switch B

```
<SW7750> system-view
[SW7750] rrpp domain 1
[SW7750-rrpp-domain-1] control-vlan 4092
[SW7750-rrpp-domain-1] ring 1 node-mode transit primary-port Gigabit
Ethernet2/0/1 secondary-port GigabitEthernet2/0/2 level 0
[SW7750-rrpp-domain-1] ring 1 enable
[SW7750-rrpp-domain-1] quit
[SW7750] rrpp enable
```

- Configure Switch C

```
<SW7750> system-view
[SW7750] rrpp domain 1
[SW7750-rrpp-domain-1] control-vlan 4092
[SW7750-rrpp-domain-1] ring 1 node-mode transit primary-port Gigabit
```

```
Ethernet2/0/1 secondary-port GigabitEthernet2/0/2 level 0
[SW7750-rrpp-domain-1] ring 1 enable
[SW7750-rrpp-domain-1] quit
[SW7750] rrpp enable
```

- Configure Switch D

```
<SW7750> system-view
[SW7750] rrpp domain 1
[SW7750-rrpp-domain-1] control-vlan 4092
[SW7750-rrpp-domain-1] ring 1 node-mode transit primary-port Gigabit
Ethernet2/0/1 secondary-port GigabitEthernet2/0/2 level 0
[SW7750-rrpp-domain-1] ring 1 enable
[SW7750-rrpp-domain-1] quit
[SW7750] rrpp enable
```

After the configuration, you can use the **display** command to view the RRPP configuration and packet statistics.

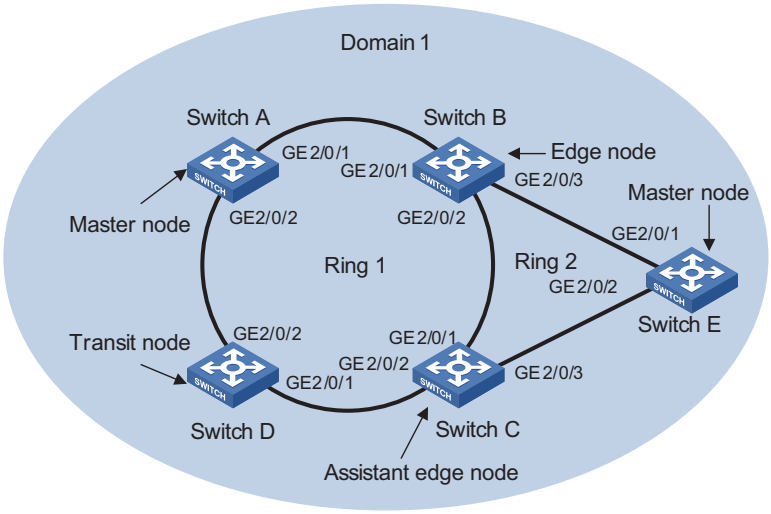
Intersectant Ring Network Configuration Example

Network requirements

- Switch A, Switch B, Switch C, Switch D and Switch E constitute RRPP domain 1
- VLAN 4092 is the control VLAN of RRPP domain 1
- Switch A, Switch B, Switch C and Switch D constitute primary ring 1.
- Switch B, Switch C and Switch E form the subring 2.
- Switch A serves as the master node of the primary ring, GigabitEthernet2/0/1 as the primary port, and GigabitEthernet2/0/2 as the secondary port.
- Switch E serves as the master node of the subring, its GigabitEthernet2/0/1 is the primary port, and its GigabitEthernet2/0/2 is the secondary port.
- Switch B serves as a transit node of the primary ring and the edge node of the subring, its GigabitEthernet2/0/2 is the common port, and its GigabitEthernet2/0/3 is the edge port.
- Switch C serves as a transit node of the primary ring and an assistant edge node of the subring, its GigabitEthernet2/0/1 is a common port, and its GigabitEthernet2/0/3 is an edge port.
- Switch D serves as a transit node of the primary ring, its GigabitEthernet2/0/1 is the primary port, and its GigabitEthernet2/0/2 is the secondary port.
- The default values are used for the timer on the primary ring and the subring.

Network diagram

Figure 255 Network diagram for intersectant ring topology



Configuration procedure

CAUTION: *Make sure that the switch ports connecting the Ethernet rings have been configured as trunk ports. All ports allow data VLAN packets to pass. And STP has been disenabled on all the ports connecting the Ethernet rings.*

- Configure Switch A

```
<SW7750> system-view
[SW7750] rrpp domain 1
[SW7750-rrpp-domain-1] control-vlan 4092
[SW7750-rrpp-domain-1] ring 1 node-mode master primary-port GigabitE
thernet2/0/1 secondary-port GigabitEthernet2/0/2 level 0
[SW7750-rrpp-domain-1] ring 1 enable
[SW7750-rrpp-domain-1] quit
[SW7750] rrpp enable
```

- Configure Switch B

```
<SW7750> system-view
[SW7750] rrpp domain 1
[SW7750-rrpp-domain-1] control-vlan 4092
[SW7750-rrpp-domain-1] ring 1 node-mode transit primary-port Gigabit
Ethernet2/0/1 secondary-port GigabitEthernet2/0/2 level 0
[SW7750-rrpp-domain-1] ring 2 node-mode edge common-port GigabitEthe
rnet 2/0/2 edge-port GigabitEthernet 2/0/3
[SW7750-rrpp-domain-1] ring 1 enable
[SW7750-rrpp-domain-1] ring 2 enable
[SW7750-rrpp-domain-1] quit
[SW7750] rrpp enable
```

- Configure Switch C

```
<SW7750> system-view
[SW7750] rrpp domain 1
[SW7750-rrpp-domain-1] control-vlan 4092
[SW7750-rrpp-domain-1] ring 1 node-mode transit primary-port Gigabit
Ethernet2/0/1 secondary-port GigabitEthernet2/0/2 level 0
[SW7750-rrpp-domain-1] ring 2 node-mode assistant-edge common-port G
```

```
igabitEthernet 0/1 edge-port GigabitEthernet 2/0/3
[SW7750-rrpp-domain-1] ring 1 enable
[SW7750-rrpp-domain-1] ring 2 enable
[SW7750-rrpp-domain-1] quit
[SW7750] rrpp enable
```

- Configure Switch D

```
<SW7750> system-view
[SW7750] rrpp domain 1
[SW7750-rrpp-domain-1] control-vlan 4092
[SW7750-rrpp-domain-1] ring 1 node-mode transit primary-port Gigabit
Ethernet2/0/1 secondary-port GigabitEthernet2/0/2 level 0
[SW7750-rrpp-domain-1] ring 1 enable
[SW7750-rrpp-domain-1] quit
[SW7750] rrpp enable
```

- Configure Switch E

```
<SW7750> system-view
[SW7750] rrpp domain 1
[SW7750-rrpp-domain-1] control-vlan 4092
[SW7750-rrpp-domain-1] ring 2 node-mode master primary-port GigabitE
thernet2/0/1 secondary-port GigabitEthernet2/0/2 level 1
[SW7750-rrpp-domain-1] ring 2 enable
[SW7750-rrpp-domain-1] quit
[SW7750] rrpp enable
```

After the configuration, you can use the **display** command to view the RRPP configuration and packet statistics.

83 TELNET PROTECTION CONFIGURATION

Introduction

The Telnet protection function is used to protect Telnet packets, SNMP packets, and ICMP packets from the specific source IP addresses in the case of attacks against the network or high CPU utilization.

Telnet protection comes in global Telnet protection, special ARP Telnet protection, and default-route Telnet protection. Global Telnet protection is the highest in priority; then comes special ARP Telnet protection and default-route Telnet protection is the lowest in priority.

After you configure global Telnet protection, all the Layer-3 interfaces are protected. You can also configure special ARP Telnet protection to protect specified Layer-3 interfaces. If the default route exists, you can enable special ARP Telnet protection on the gateway of the network segment where the next hop of the default route resides through enabling default-route Telnet protection. By default, default-route Telnet protection is disabled.

Before configuring Telnet protection, you need to enable Telnet, SNMP, and ICMP protection respectively. You can configure Telnet protection, SNMP protection, and ICMP protection for only the packets of the specific source IP addresses.



CAUTION: *After the network address translation (NAT) function is enabled,*

- *You cannot configure global Telnet protection.*
- *You cannot configure special ARP Telnet protection for the Layer-3 interface where NAT resides.*
- *You cannot configure default-route Telnet protection.*

Telnet Protection Configuration

Configuring Telnet Protection

Table 710 Configure Telnet protection

Operation	Command	Description
Enter system view	**system-view**	-
Enable Telnet protection	**attack-protection telnet** [*ip-address*]	Required If you use this command with the *ip-address* parameter, you can protect the packets that match this source IP address only.

Table 710 Configure Telnet protection

Operation	Command	Description
Enable global Telnet protection or special ARP Telnet protection	**attack-protection** [*ip-address*]	Required If you use this command with the *ip-address* parameter, you can protect the specified Layer-3 interfaces.

Configuring SNMP Protection

Table 711 Configure SNMP protection

Operation	Command	Description
Enter system view	**system-view**	-
Enable SNMP protection	**attack-protection snmp** [*ip-address*]	Required If you use this command with the *ip-address* parameter, you can protect the packets that match this source IP address only
Enable global Telnet protection or special ARP Telnet protection	**attack-protection** [*ip-address*]	Required If you use this command with the *ip-address* parameter, you can protect the specified Layer-3 interfaces.

Configuring ICMP Protection

Table 712 Configure ICMP protection

Operation	Command	Description
Enter system view	**system-view**	-
Enable ICMP protection	**attack-protection icmp** [*ip-address*]	Required If you use this command with the *ip-address* parameter, you can protect the packets that match this source IP address only
Enable global Telnet protection or special ARP Telnet protection	**attack-protection** [*ip-address*]	Required If you use this command with the *ip-address* parameter, you can protect the specified Layer-3 interfaces.

Configuring Default-route Telnet Protection

Table 713 Configuring default-route Telnet protection

Operation	Command	Description
Enter system view	**system-view**	-
Enable default-route Telnet protection	**undo attack-protection disable-defaultroute**	Required By default, default-route Telnet protection is disabled.

84 SMART LINK CONFIGURATION

Smart Link Overview

As shown in Figure 256, dual-uplink networking is widely applied currently. Usually, spanning tree protocol (STP) is used to implement link redundancy backup in the network. However, STP is not suitable for users with a high demand for convergence time. Smart Link can achieve active/standby link redundancy backup and fast convergence to meet the user demand.

Smart Link has the following features:

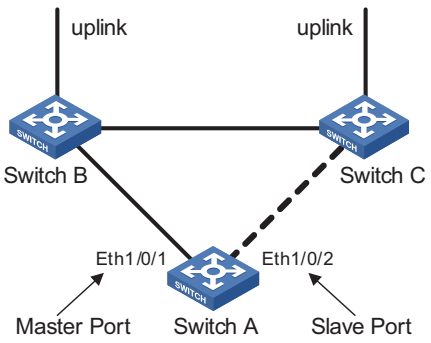
- Active/standby backup for dual-uplink networking
- Simple configuration and operation

Basic Concepts in Smart Link

Smart Link group

A Smart Link group consists of two member ports, one master port and one slave port. Normally, only one port (master or slave) is active, and the other port is blocked, that is, in the standby state. When link failure occurs on the port in active state, the Smart Link group will block the port automatically and turn standby state to active state on the blocked port.

Figure 256 Network diagram of Smart Link



In Figure 256, Ethernet2/0/1 and Ethernet2/0/2 on Switch A are two member ports of a Smart Link group.

Master port

The master port can be either an Ethernet port or a manually-configured or static LACP aggregation group. For example, you can configure Ethernet2/0/1 of switch A in Figure 256 as the master port through the command line.

Slave port

The slave port can be either an Ethernet port or a manually-configured or static LACP aggregation group. For example, you can configure Ethernet2/0/2 of switch A in Figure 256 as the slave port through the command line.

Flush message

When a forwarding link fails, the device will switch the traffic to the blocked standby link. The former forwarding entries of each device in the network are no longer suitable for the new topology, so MAC address forwarding entries and ARP entries must be updated throughout the network. In this case, the Smart Link group sends flush messages to notify other devices to refresh MAC address forwarding entries and ARP entries.

Control VLAN for sending flush messages

This control VLAN sends flush messages. When link switching occurs, the device (Switch A in Figure 256) broadcasts flush messages in this control VLAN.

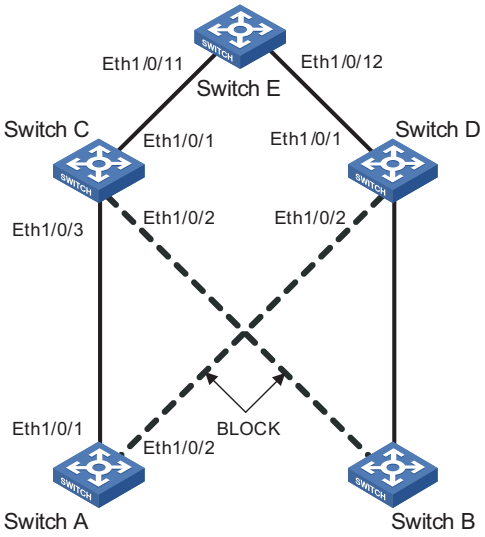
Control VLAN for receiving flush messages

This control VLAN is used for receiving and processing flush messages. When link switching occurs, the devices (Switch B and Switch C in Figure 256) receive and process flush messages of this control VLAN, and then refresh MAC forwarding table entries and ARP entries.

- *Currently, the member ports of a Smart Link group cannot be dynamic link aggregation groups.*
- *If the master port or slave port of a Smart Link group is a link aggregation group, you cannot remove this link aggregation group directly or change the aggregation group into a dynamic aggregation group. Before removing this aggregation group, you must unbind the link aggregation group from the Smart Link.*

Operating Mechanism of Smart Link

Figure 257 Network diagram of Smart Link operating mechanism



As shown in Figure 257, Ethernet2/0/1 on Switch A is active and Ethernet2/0/2 on Switch A is blocked. When the link connected to Ethernet2/0/1 fails, Ethernet2/0/1 is blocked automatically, and the state of Ethernet2/0/2 turns to active state.

- When link switching occurs in the Smart Link group, MAC forwarding entries and ARP entries of each device in the network may be out of date. In order to guarantee correct packet transmission, you must enable the Smart Link device to send flush messages to notify the other devices in the network to refresh their own MAC forwarding entries and ARP entries. In this case, all the uplink devices must be capable of identifying flush messages from the Smart Link group and refreshing MAC forwarding entries and ARP entries.
- On a Smart Link-enabled device, if a port is blocked due to link failure, the port remains blocked after the link recovers from the failure, and does not preempt the traffic resource. Therefore, the traffic stays stable. The port does not come into the forwarding state until the next link switching.

Configuring Smart Link



Before configuring a member port of a Smart Link group, you must:

- *Disable the port to avoid loops, thus preventing broadcast storm.*
- *Disable STP on the port.*

After completing the configuration, you need to enable the Ethernet ports disabled before configuring the Smart Link group.

Configuration Tasks

Table 714 Smart Link configuration tasks

Task		Remarks
"Configuring a Smart Link Device" on page 925	Create a Smart Link group	Required
	Add member ports to the Smart Link group	
	Enable the function of sending flush messages in the specified control VLAN	
"Configuring Associated Devices" on page 926	Enable the function of processing flush messages received from the specified control VLAN	Required

Configuring a Smart Link Device

A Smart Link device refers to a device on which Smart Link is enabled and a Smart Link group is configured, and that sends flush messages from the specified control VLAN. A member port of a Smart Link group can be either an Ethernet port or a manually-configured or static LACP aggregation group. You can configure a port or a link aggregation group as a member of a Smart Link group.

Table 715 Configure Smart Link (with ports as the members of the Smart Link group)

Operation		Command	Remarks
Enter system view		**system-view**	-
Create a Smart Link group and enter Smart Link group view		**smart-link group** *group-id*	Required
Enable the function of sending flush messages in the specified control VLAN		**flush enable control-vlan** *vlan-id*	Required By default, no control VLAN for sending flush messages is specified.
Configure a port as a Smart Link group member	Smart Link group view	**port** *interface-type interface-number* { **master** | **slave** }	Required Use either approach
	Ethernet port view	**quit**	
		interface *interface-type interface-number*	
		port smart-link group *group-id* { **master** | **slave** }	

Table 716 Configure Smart Link (with link aggregation groups are the members of the Smart Link group)

Operation	Command	Remarks
Enter system view	**system-view**	-
Create a Smart Link group and enter Smart Link group view	**smart-link group** *group-id*	Required
Configure a link aggregation group as a member of the Smart Link group	**link-aggregation group** *group-id* { **master** | **slave** }	Optional
Enable the function of sending flush messages in the specified control VLAN	**flush enable control-vlan** *vlan-id*	Optional By default, no control VLAN for sending flush messages is specified.

Configuring Associated Devices

An associated device mentioned in this document refers to a device that supports Smart Link and locally configured to process flush messages received from the specified control VLAN so as to work with the corresponding Smart Link device. As shown in Figure 257, all the devices including Switch C, Switch D, and Switch E on the active and backup links connecting the Smart Link device (Switch A) and the target uplink device (Switch E) are all associated devices.

However, you do not have to enable all the ports of an associated device to process flush messages received from the specified control VLAN. You need to enable this function only on the ports that are on the active and backup links connecting the Smart Link device and the target device. As shown in Figure 257, you need to enable this function on Ethernet 2/0/2 and Ethernet 2/0/3 of Switch C, Ethernet 2/0/2 and Ethernet 2/0/3 of Switch D, and Ethernet 12/0/1 and Ethernet 2/0/12 of Switch E.

Table 717 Enable the specified port to process flush messages received from the specified control VLAN

Operation		Command	Remarks
Enter system view		**system-view**	-
Enable the specified port(s) to process flush messages received from the control VLAN	System view	**smart-link flush enable control-vlan** *vlan-id* **port** *interface-type interface-number* [**to** *interface-type interface-number*]	Required, use either approach. By default, no control VLAN for receiving flush messages is specified.
	Ethernet port view	**interface** *interface-type interface-number*	
		smart-link flush enable control-vlan *vlan-id*	

Precautions When configuring Smart Link, pay attention to the following points:

1 A port or a link aggregation group cannot serve as a member port for two Smart Link groups. On the other hand, a port or a link aggregation group cannot serve as a member for a Smart Link group and a Monitor Link group at the same time.

2 STP cannot be enabled on the member ports of a Smart Link group. An STP-enabled port or a link aggregation group with an STP-enabled port cannot serve as a member port for a Smart Link group.

3 A Smart Link/Monitor Link group with members cannot be deleted.

4 Smart Link/Monitor Link is mutually exclusive with remote port mirroring.

5 When you copy a port, the Smart Link/Monitor Link group member information configured on the port will not be copied to other ports.

6 If a single port is specified as a member of a Smart Link/Monitor Link group, you cannot execute the **lacp enable** command on this port or add this port into other dynamic link aggregation groups, because these operations will make this port become a link aggregation group member.

7 If no control VLAN is configured for flush message processing, the device will forward received flush messages without processing them.

8 If the control VLAN for receiving flush messages configured on an associated device is different than the one for sending flush messages configured on the corresponding Smart Link device, the device will forward received flush messages without processing them.

9 In the static or manual link aggregation group which serves as a Smart Link group member, if a member port can process flush messages, this function cannot be synchronized to the other ports in the aggregation group automatically, that is, the other member ports in the aggregation group cannot process flush messages. The function of processing flush messages must be manually configured for each port in the aggregation group.

10 The VLAN configured as a control VLAN to send and receive flush messages must exist. You cannot directly remove the control VLAN. When a dynamic VLAN is configured as the control VLAN for the Smart Link group, this VLAN will become a static VLAN, and the prompt information is displayed.

Displaying and Debugging Smart Link

After the above-mentioned configuration, you can use the following **display** commands in any view to view the Smart Link group information and the statistics information of flush messages received and processed by current device, so as to verify the configuration.

Use the **reset** command in user view to clear flush message statistics.

Table 718 Display and debug Smart Link

Operation	Command	Remarks
Display the information of a Smart Link group	**display smart-link group** { *group-id* | **all** }	You can execute the **display** command in any view.
Display the statistics information of flush messages received and processed by the current device	**display smart-link flush**	
Clear flush message statistics	**reset smart-link packets counter**	You can execute the **reset** command in user view.

Smart Link Configuration Example

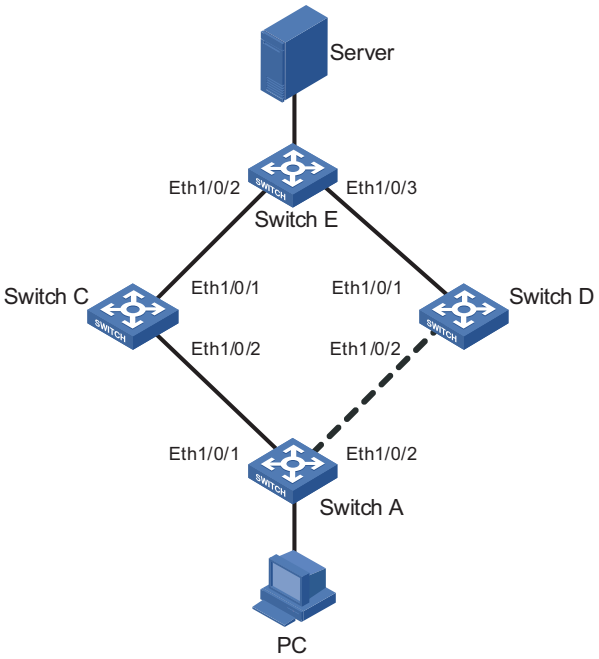
Implementing Link Redundancy Backup

Network requirements

As shown in Figure 258, Switch A is an 3Com Switch 7750 Ethernet switch. Switch C, Switch D and Switch E support Smart Link. Configure Smart Link feature to provide remote PCs with reliable access to the server.

Network diagram

Figure 258 Network diagram for Smart Link configuration



Configuration procedure

1 Configure a Smart Link group on Switch A and configure member ports for it. Enable the function of sending flush messages in Control VLAN 1.

Enter system view.

```
<switchA> system-view
```

Enter Ethernet port view. Disable STP on Ethernet2/0/1 and Ethernet2/0/2.

```
[SwitchA] interface Ethernet 2/0/1
[SwitchA-Ethernet2/0/1] stp disable
[SwitchA-Ethernet2/0/1] quit
[SwitchA] interface Ethernet 2/0/2
[SwitchA-Ethernet2/0/2] stp disable
```

Return to system view.

```
[SwitchA-Ethernet2/0/2] quit
```

Create Smart Link group 1 and enter the corresponding Smart Link group view.

```
[SwitchA] smart-link group 1
```

Configure Ethernet2/0/1 as the master port and Ethernet2/0/2 as the slave port for Smart Link group 1.

```
[SwitchA-smlk-group1] port Ethernet 2/0/1 master
[SwitchA-smlk-group1] port Ethernet 2/0/2 slave
```

Configure to send flush messages within VLAN 1.

```
[SwitchA-smlk-group1] flush enable control-vlan 1
```

2 Enable the function of processing flush messages received from VLAN 1 on Switch C.

Enter system view.

```
<SwitchC> system-view
```

Enable the function of processing flush messages received from VLAN 1 on Ethernet 2/0/2.

```
<SwitchC> smart-link flush enable control-vlan 1 port Ethernet 2/0/2
```

3 Enable the function of processing flush messages received from VLAN 1 on Switch D.

Enter system view.

```
<SwitchD> system-view
```

Enable the function of processing flush messages received from VLAN 1 on Ethernet 2/0/2.

```
[SwitchD] smart-link flush enable control-vlan 1 port Ethernet 2/0/2
```

4 Enable the function of processing flush messages received from VLAN 1 on Switch E.

Enter system view.

```
<SwitchE> system-view
```

Enable the function of processing flush messages received from VLAN 1 on Ethernet 2/0/2 and Ethernet 2/0/3.

```
[SwitchE] smart-link flush enable control-vlan 1 port Ethernet 2/0/2
 to Ethernet 2/0/3
```

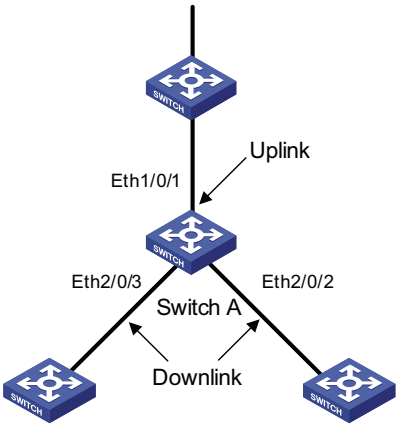
85 MONITOR LINK CONFIGURATION

Introduction to Monitor Link

Monitor Link is a collaboration scheme introduced to complement for Smart Link. It is used to monitor uplink and to perfect the backup function of Smart Link.

A monitor Link consists of an uplink port and one or multiple downlink ports. When the link for the uplink port of a Monitor Link group fails, all the downlink ports in the Monitor Link group are forced down. When the link for the uplink port recovers, all the downlink ports in the group are re-enabled.

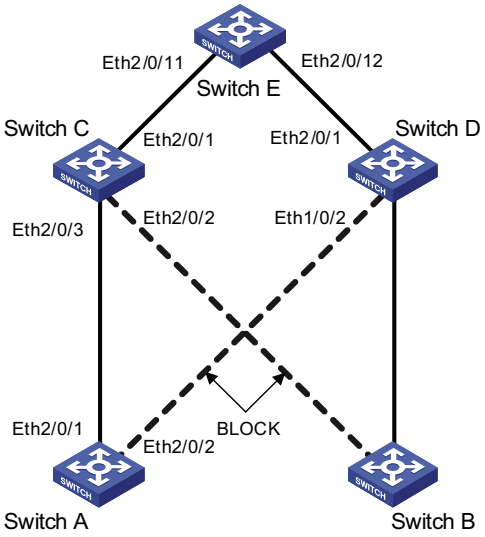
Figure 259 Network diagram for a Monitor Link group implementation



As shown in Figure 259, the Monitor Link group configured on the device Switch A consists of an uplink port (Ethernet2/0/1) and two downlink ports (Ethernet2/0/2 and Ethernet2/0/3). A member port can be an Ethernet port, static LACP aggregation group, manual link aggregation group, or Smart Link group. A Smart Link group can serve as the uplink port only.

How Monitor Link Works

Figure 260 Network diagram for a Monitor Link group implementation



As shown in Figure 260, the devices Switch C and Switch D are connected to the uplink device Switch E. Switch C is configured with a Monitor Link group, where Ethernet2/0/1 is the uplink port, while Ethernet2/0/2 and Ethernet2/0/3 are the downlink ports. Switch A is configured with a Smart Link group, where Ethernet2/0/1 is the master port and Ethernet2/0/2 is the slave port.

- If Switch C is not configured with Monitor Link group, when the link for the uplink port Ethernet2/0/1 on Switch C fails, the links in the Smart Link group are not switched because the link for the master port Ethernet2/0/1 of Switch A configured with Smart Link group operates normally. Actually, however, the traffic on Switch A cannot be up-linked to Switch E through the link of Ethernet2/0/1.
- If Switch C is configured with Monitor Link group and Monitor Link group detects that the link for the uplink port Ethernet2/0/1 fails, all the downlink ports in the group are shut down; therefore, Ethernet2/0/3 on Switch C is blocked. Now, Smart Link group configured on Switch A detects that a link fault occurs on the master port Ethernet2/0/1. Then, Smart Link immediately activates the slave port Ethernet2/0/2 so that traffic is switched to the backup link.



- *Currently, member ports of a Monitor Link group cannot be dynamic link aggregation groups.*
- *If the uplink or downlink port in the Monitor Link group is a link aggregation group, you cannot directly delete this aggregation group or change this aggregation group into a dynamic aggregation group. To delete this aggregation group, you must first unbind this aggregation group from the Monitor Link.*

Configuring Monitor Link



Before configuring a Monitor Link group, you must create a Monitor Link group and configure member ports for it. A Monitor Link group consists of an uplink port

and one or multiple downlink ports. The uplink port can be a manually-configured or static LACP link aggregation group, an Ethernet port, or a Smart Link group. The downlink ports can be manually-configured link aggregation groups or static LACP link aggregation groups, or Ethernet ports.

Configuration Tasks

Table 719 Monitor Link configuration tasks

Task	Remarks
"Creating a Monitor Link Group" on page 933	Required
"Configuring the Uplink Port" on page 933	Required
"Configuring a Downlink Port" on page 933	Required

Creating a Monitor Link Group

Table 720 Create a Monitor Link group

Operation	Command	Remarks
Enter system view	**system-view**	-
Create a Monitor Link group	**monitor-link group** *group-id*	Required

Configuring the Uplink Port

Table 721 Configure the uplink port

Operation			Command	Remarks
Enter system view			**system-view**	-
Enter the specified Monitor Link group view			**monitor-link group** *group-id*	-
Configure the uplink port for the Monitor Link group	Configure the specified link aggregation group as the uplink port of the Monitor Link group		**link-aggregation group** *group-id* **uplink**	Required Use any of the three approaches
	Configure the specified Smart Link group as the uplink port of the Monitor Link group		**smart-link group** *group-id* **uplink**	
	Configure the specified Ethernet port as the uplink port of the Monitor Link group	Monitor Link group view	**port** *interface-type interface-number* **uplink**	
		Ethernet port view	**quit**	
			interface *interface-type interface-number*	
			port monitor-link group *group-id* **uplink**	

Configuring a Downlink Port

Table 722 Configure a downlink port

Operation	Command	Remarks
Enter system view	**system-view**	-
Enter the specified Monitor Link group view	**monitor-link group** *group-id*	Required

Table 722 Configure a downlink port

Operation			Command	Remarks
Configure a downlink port for the Monitor Link group	Configure the specified link aggregation group as a downlink port of the Monitor Link group		**link-aggregation group** *group-id* **downlink**	Required Use either approach
	Configure the specified Ethernet port as a downlink port of the Monitor Link group	Monitor Link group view	**port** *interface-type interface-number* **downlink**	
		Ethernet port view	**quit**	
			interface *interface-type interface-number*	
			port monitor-link group *group-id* **downlink**	

CAUTION:

- *A Smart Link/Monitor Link group with members cannot be deleted. A Smart Link group as a Monitor Link group member cannot be deleted.*
- *The Smart Link/Monitor Link function and the remote port mirroring function are incompatible with each other.*
- *If a single port is specified as a Smart Link/Monitor Link group member, do not use the **lacp enable** command on the port or add the port to another dynamic link aggregation group because doing so will cause the port to become an aggregation group member.*
- *Using the copy command on a port does not copy the Smart Link/Monitor Link group member information configured on the port to any other port.*

Displaying Monitor Link Configuration

After the above-mentioned configuration, you can use the **display** command in any view to display the information about Monitor Link, so as to verify configuration result.

Table 723 Display Monitor Link configuration

Operation	Command	Remarks
Display the information about one or all Monitor Link groups	display monitor-link group { *group-id* | all }	You can use the **display** command in any view.

Monitor Link Configuration Example

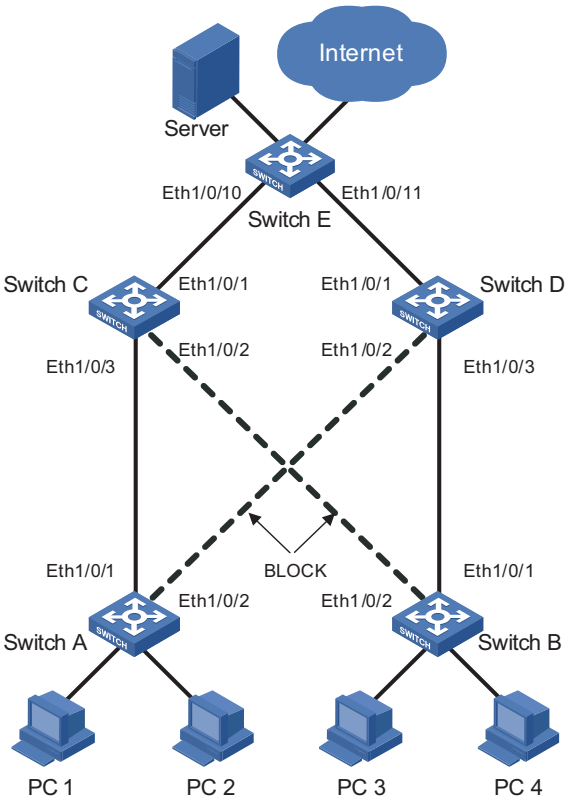
Implementing Collaboration Between Smart Link and Monitor Link

Network requirements

As shown in Figure 261, the PCs access the server and Internet through the switch. Configure Smart Link and Monitor Link to prevent the PCs from failing to access the server and Internet due to uplink link or port failure.

Network diagram

Figure 261 Network diagram for Monitor Link configuration



Configuration procedure

1 Enable Smart Link on Switch A and Switch B to implement link redundancy backup. Perform the following configuration on Switch A. The configuration on Switch B is the same as on Switch A.

Enter system view.

```
<switchA> system-view
```

Enter Ethernet port view. Disable STP on Ethernet2/0/1 and Ethernet2/0/2.

```
[SwitchA] interface Ethernet 2/0/1
[SwitchA-Ethernet2/0/1] stp disable
[SwitchA-Ethernet2/0/1] quit
[SwitchA] interface Ethernet 2/0/2
[SwitchA-Ethernet2/0/2] stp disable
```

Return to system view.

```
[SwitchA-Ethernet2/0/2] quit
```

Create Smart Link group 1 and enter Smart Link group view.

```
[SwitchA] smart-link group 1
```

Configure Ethernet2/0/1 as the master port of the Smart Link group and Ethernet2/0/2 as the slave port.

```
[SwitchA-smlk-group1] port Ethernet 2/0/1 master
[SwitchA-smlk-group1] port Ethernet 2/0/2 slave
```

Configure to send flush messages in VLAN 1.

```
[SwitchA-smlk-group1] flush enable control-vlan 1
```

2 Enable Monitor Link on Switch C and Switch D and enable the function of processing flush messages received from VLAN 1. Perform the following configuration on Switch C. The operation procedure on Switch D is the same as that performed on Switch C.

Enter system view.

```
<SwitchC> system-view
```

Create Monitor Link group 1 and enter Monitor Link group view

```
[SwitchC] monitor-link group 1
```

Configure Ethernet2/0/1 as the uplink port of the Monitor Link group and Ethernet2/0/2 and Ethernet2/0/3 as the downlink ports.

```
[SwitchC-mtlk-group1] port Ethernet 2/0/1 uplink
[SwitchC-mtlk-group1] port Ethernet 2/0/2 downlink
[SwitchC-mtlk-group1] port Ethernet 2/0/3 downlink
```

Return to system view. Enable the function of processing flush messages received from VLAN 1 on Ethernet2/0/2 and Ethernet2/0/3.

```
[SwitchC-mtlk-group1] quit
[SwitchC] smart-link flush enable control-vlan 1 port Ethernet 2/0/2
 to Ethernet 2/0/3
```

3 Enable the function of processing flush messages received from VLAN 1 on Ethernet 2/0/10 and Ethernet 2/0/11 of Switch E.

Enter system view.

```
<SwitchE> system-view
```

Enable the function of processing flush messages received from VLAN 1 on Ethernet 2/0/10 and Ethernet 2/0/11.

```
[SwitchE] smart-link flush enable control-vlan 1 port Ethernet 2/0/1
0 to Ethernet 2/0/11
```

86 CONFIGURING HARDWARE-DEPENDENT SOFTWARE

Configuring Boot ROM Upgrade with App File

By enabling Boot ROM to upgrade together with the app file, you can ensure that the Boot ROM versions of the current Fabric and service modules can match the version of the current app file, thus avoiding invalid feature implementation caused by mismatching.

Two upgrade types are available:

- The current startup file as the upgrade file for Boot ROM
- The specified App file as the upgrade file for Boot ROM

Boot ROM Upgrade Configuration

Table 724 Configure Boot ROM upgrade

Operation	Command	Description
Set the current startup file as the upgrade file for Boot ROM	**boot bootrom default** [**slot** *slot-number-list*]	Optional
Set the specified App file as the upgrade file for Boot ROM	**boot bootrom** *file-url* [**slot** *slot-number-list*]	Optional
Set the primary startup file at next booting and use it to upgrade the Boot ROM	**boot boot-loader primary** *file-url*	Optional

CAUTION:

- *If you do not specify a slot number in the boot bootrom command, the system upgrades all normal modules in position by default.*
- *After you specify the primary startup file for the next booting, the system upgrades all normal modules in the process of upgrading Boot ROM. You need also to confirm the upgrade operation in the upgrade process.*

Boot ROM Upgrade Configuration Example

Network requirements

- Use the current startup file to upgrade the Boot ROMs of all normal I/O Module modules in position.
- Use the specified App file (abcd.app) to upgrade the Boot ROMs of all normal I/O Module modules in position.
- Specify the App file abcd.app as the primary startup file for next booting and use it to upgrade the Boot ROMs.

Configuration example

Use the current startup file to upgrade the Boot ROMs of all normal I/O Module modules in position.

```
<SW7750> boot bootrom default
```

Use the specified App file (**abcd.app**) to upgrade the Boot ROMs of slot 1 I/O Module modules in position.

```
<SW7750> boot bootrom abcd.app
```

Specify the App file **abcd.app** as the primary startup file for next booting.

```
<SW7750> boot boot-loader primary abcd.app
```

Configuring Inter-Card Link State Adjustment

Introduction

The inter-card link state adjustment function is designed to improve the adaptability of the inter-card links in a Switch 7750. It enables you to set the mode in which inter-card links are established as needed.

An inter-card link refers to the internal links between the Fabric and all the service modules of an Ethernet switch.

Inter-card links can be established in one of the following two modes:

- Auto-negotiation mode, where inter-card links are established through negotiation to improve the adaptability and stability. This mode is based on the corresponding Ethernet standards. By default, the Fabric and the service modules in a Switch 7750 Ethernet switch negotiate to establish 1000 Mbps links in between.
- Fix mode, where 1000 Mbps links are established between the Fabric and the service modules without negotiation. Therefore, the time for negotiation is saved. For the switches operating as network nodes, establishing inter-card links in this mode improves the response speed and reduces the influence on access devices when module switchovers occur.

Since the two modes have no affect on the performance, it is unnecessary to modify the existing configuration when you employ this function.

Inter-Card Link State Adjustment Configuration

Table 725 Configure inter-card link state adjustment

Operation	Command	Description
Enter system view	**system-view**	-
Set the mode in which inter-card links are established	**set inlink** { **auto** | **fix** }	Required By default, inter-card links are established in the auto negotiation mode

Configuring Internal Channel Monitoring

Introduction

An internal channel refers to the interface channel between the Fabric and the service modules. The Fabric sends handshake packets to each service module every second. After receiving the handshake packets, the service modules reports the result to the Fabric. In this case, the Fabric knows that the service modules are operating normally. Through this process, the Fabric can judge whether each service module in the device operates normally.

Switch 7750s support this feature. Through this feature, you can monitor internal channels.

You can also set the maximum number of times the Fabric fails to receive handshake packets. If the number of times the Fabric fails to receive handshake packets exceeds the upper limit, the switch resets the processing chip automatically. When the Fabric receives handshake packets, it resets the counter automatically.

You can also set whether to restart the service module or the switch when the number of times the Fabric fails to receive handshake packets exceeds the upper limit.

Monitoring Internal Channel Configuration

Table 726 Monitor internal channels

Operation	Command	Description
Enter system view	**system-view**	-
Enable the function of monitoring internal channels	**monitor inner-channel**	Optional
Configure to restart the service card	**monitor inner-channel reboot-lpu**	Optional
Configure to restart the switch	**monitor inner-channel reboot-switch**	Optional
Set the upper limit for resetting the chip	**monitor inner-channel upper-limit** *upper-timers*	Optional

Configuring Switch Chip Auto-reset

Introduction

In actual application, a switch may fail to process services normally due to internal channel block or because the switch chip is busy.

Switch 7750s support the function of resetting switch chips automatically. In case that the function of monitoring internal channels is enabled, when the internal channel handshake between a module and the backplane fails, the switch resets the switch chip automatically to resume the corresponding module.

When the function of resetting switch chips is disabled, even if the switch finds that the internal channel handshake fails, it cannot reset the switch chip automatically.

Switch Chip Auto-reset Configuration

Table 727 Configure switch chip auto-reset

Operation	Command	Description
Enter system view	**system-view**	-
Enable the function of monitoring internal channels	**monitor inner-channel**	Required
Enable switch chip auto-reset	**monitor slot** *slot-id* **enable**	Required By default, switch chips cannot be reset automatically when the internal channel handshake fails
Disable switch chip auto-reset	**monitor slot** *slot-id* **disable**	Optional

Configuring CPU Usage Threshold

Introduction

3Com Switch 7750 Ethernet switches are layer-2/layer-3 Ethernet switches with multiple slots and of high reliability. CPUs of Fabrics and I/O Modules can process data. In actual networking, they may receive many requests for data/packet processing at the same time due to large traffic or complicated networking. These requests occupy many CPU resources and affect network stability.

Switch 7750 Ethernet switches support CPU usage threshold configuration. When the CPU usage exceeds the configured threshold, the switch sends trap messages and log messages, according to which the network administrator can modify the switch configuration.

Switch 7750 Ethernet switches also support configuration of the CPU usage threshold of the specified module. You can specify **slot** *slot-number* to configure the CPU usage threshold for the specified module. When the CPU usage of the module in the specified slot exceeds the configured threshold, the switch sends trap messages and log messages to the network administrator.

If you set CPU thresholds for both all the modules and the specified module, the CPU threshold of the specified module is determined by the latter one. For example, if you set the CPU usage threshold of all the modules to 88 and set that of the module in slot 2 to 77, the CPU usage threshold of the module in slot 2 is 77.

CPU Usage Threshold Configuration

Table 728 Configure CPU usage threshold

Operation	Command	Description
Enter system view	**system-view**	-
Configure CPU usage threshold	**cpu-usage-threshold** *value* [**slot** *slot- id*]	Required By default, this function is disabled.